An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families

Chapter 4
An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families

Tomer Ashur and Atul Luykx

Abstract Simon and Speck are two block cipher families published in 2013 by the US National Security Agency (NSA). These block ciphers, targeting lightweight applications, were suggested in 2015 to be included in *ISO/IEC 29192-2 Information technology—Security techniques—Lightweight cryptography—Part 2: Block ciphers*. Following 3.5 years of deliberations within ISO/IEC JTC 1 they were rejected in April 2018. This chapter provides an account of the ISO/IEC standardization process for Simon and Speck.

4.1 Introduction

By their very nature, cryptographic algorithms require large-scale agreement to enable secure communication. Standardization by bodies such as ANSI, IEEE, and ISO/IEC is important means by which industries and governments achieve such agreement. The standardization process can be effective for agreeing upon trustworthy, secure, and efficient cryptographic algorithms when conducted in the open, as was the case with AES [444]. Yet opaque standardization processes lend themselves to subversion, as exemplified by Dual-EC [472].

In recent years, standardization bodies have initiated projects to understand the need for lightweight cryptographic algorithms. We shed light on the ISO/IEC standardization process, one not well understood by the general public, by delving into how cryptographic algorithms are scrutinized and determined to be fit for standardization. To this end, we present a chronological description of the events that led to removal of the NSA block ciphers Simon and Speck [64] from

T. Ashur (✉)
imec-COSIC, KU Leuven, Leuven, Belgium

TU Eindhoven, Eindhoven, The Netherlands
e-mail: tomer.ashur@esat.kuleuven.be

A. Luykx
imec-COSIC, KU Leuven, Leuven, Belgium

G. Avoine, J. Hernandez-Castro (eds.), *Security of Ubiquitous Computing Systems*,
https://doi.org/10.1007/978-3-030-10591-4_4

Table 4.1 Simon's parameters

Block size ($2n$)	Key size (mn)	Rounds (T)
32	64	32
48	72	36
	96	36
64	96	42
	128	44
96	96	52
	144	54
128	128	68
	192	69
	256	72

consideration in the ISO/IEC process, spanning 5 years from their initial public release. We aim to educate the wider public and academic community about the process which leads governments and industries to agree upon the algorithms which secure their digital communications.[1]

4.2 Simon and Speck

Simon and Speck are two block cipher families designed by the NSA and published in 2013 [64]. Each family has ten variants differing in their block- and key- sizes. Both ciphers aim to be extremely efficient on resource constrained platforms, with Simon targeting hardware implementation and Speck software implementation.

4.2.1 Simon

A member of the Simon family is denoted Simon$2n/mn$ where $2n$ is the block size and mn is the key size. For a list of block- and key-size pairs see Table 4.1. All variants use a balanced Feistel structure iterating a simple round function using only XOR's, bitwise AND's and cyclic bit rotations. Simon's round function is depicted in Fig. 4.1.

For all variants, the key schedule is an LFSR operating on m words.

The number of rounds for each variant, which was a big source of contention during the standardization process, as well as the round dependent constants, can also be found in Table 4.1.

[1]The authors have been actively participating in the discussions surrounding this project as ISO/IEC JTC 1/SC 27/WG 2 experts. This chapter is an account of their personal experiences.

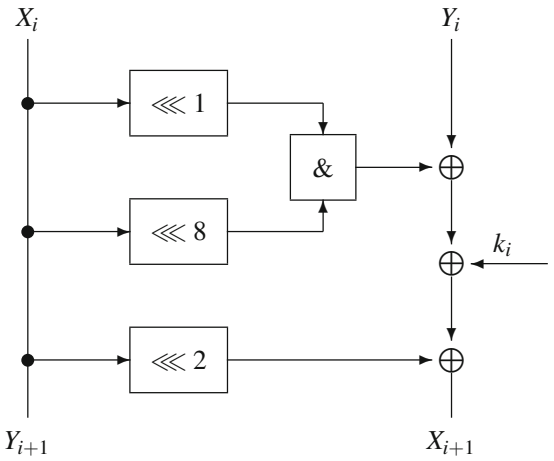

Fig. 4.1 One round of Simon (without the final swap operation)

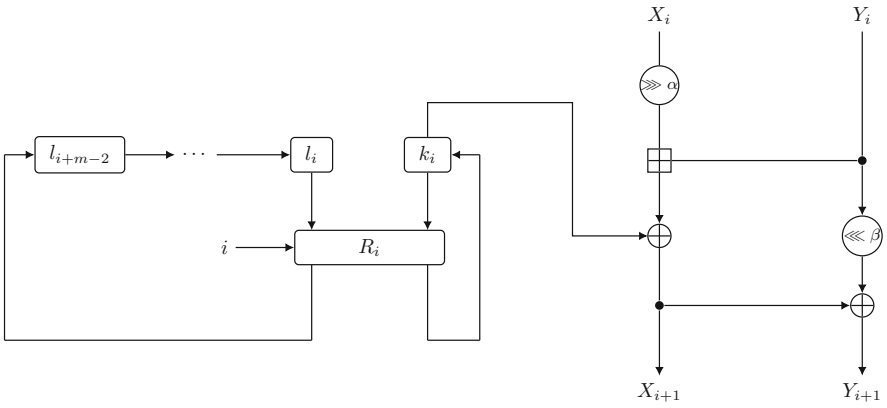

Fig. 4.2 One round of Speck and its key schedule

4.2.2 Speck

Similar to Simon the Speck family includes ten variants, differing in their block- and key- sizes. A member is denoted Speck$2n/mn$ where $2n$ is the block size and mn is the key size. Speck builds on the ARX design paradigm and the cipher is composed of three operations: modular Addition, Rotation, and XOR (hence the name ARX).

While efficient in software, ARX operations are known to have slow diffusion. Usually, this slow diffusion mandates employing a large number of rounds (see e.g., [214]) to be secure. However, as discussed in the sequel, the designers argued that they have a good understanding of the cipher's diffusion and settled for a relatively small number of rounds.

Table 4.2 Speck's parameters

Block size ($2n$)	Key size (mn)	(α, β)	Rounds (T)
32	64	(7, 2)	22
48	72	(8, 3)	22
	96	(8, 3)	23
64	96	(8, 3)	26
	128	(8, 3)	27
96	96	(8, 3)	28
	144	(8, 3)	29
128	128	(8, 3)	32
	192	(8, 3)	33
	256	(8, 3)	34

To reduce implementation size, the designers reuse Speck's round function for the key schedule, feeding in the round number as the round key and outputting one subkey word in every round. Depicted in Fig. 4.2 are the round function and the key schedule for Speck. The pairs of possible block- and key- sizes, and the rotation constants α and β for each variant are listed in Table 4.2.

4.3 Simon and Speck's "Design Rationale"

A standard practice in modern block cipher design is to provide a design rationale explaining the design decisions (e.g., the choices of round constants, number of rounds, rotation amounts, etc.), and the expected security of the new algorithm. There is no particular structure to a design rationale, but it usually includes a description of the attacks the designer attempted to apply against the algorithm, and some reasoning about why the designer believes the algorithm to be secure (e.g., using the wide-trail strategy). If the cipher has additional features (such as being an involution) they are also described and explained in the design rationale.

The purpose of the design rationale is twofold. First, it allows a cryptanalyst to quickly discard attacks that have been attempted and ruled out by the designer. Secondly, it provides a general idea about how secure the algorithm should be. Once new attacks are found against an algorithm they can be compared with the expected security reported by the designer to see how serious they are.

An important component to establishing confidence in a new algorithm's security is the teamwork between the designer and third party cryptanalysts. While the designer has the "home advantage" of understanding the internals of their algorithm, the cryptanalyst enjoys an unbiased view that allows them to see things that might have been overlooked by the designer.

This is why it came as a surprise that the NSA chose not to provide any security design rationale for their algorithms. The lure of analyzing newly released NSA-ciphers proved tempting for many, as the vacuum the NSA left behind was quickly filled with third party analysis such as those in [5, 6, 18, 19, 183].

As a result of substantial resistance to their attempts to standardize Simon and Speck in ISO—discussed further below—the designers finally offered to ISO what they called a "design rationale" in April 2017. As per the request from ISO experts, this so-called design rationale was made public to the crypto-community via the ePrint repository in June 2017 [66].[2] The purpose of releasing this design rationale is stated in Sect. 4.4:

> A desire has been expressed that we publish our analysis of Simon and Speck, and we certainly understand the wish to have insight into our analysis. Therefore, we would like to address that here. We will begin by addressing how we as the design team considered the standard block cipher attacks and their applicability to the security of the SIMON and SPECK design.

However, the joy of finally having a design rationale was short-lived. While the document is heavy on selling the algorithms' efficiency, the security part of the design rationale is practically non-existent. A careful reading of [66, Sec. 4] reveals that it includes no new information regarding the algorithms' security, and merely cites publicly known third party analysis. In particular, three caveats which we now describe in detail raised questions about whether this so-called design rationale was published in good faith.

4.3.1 Lack of New Information

Rather than explaining the attacks the design team attempted, the authors quote the work of others without committing to any particular security claim. The so-called security analysis opens with:

> As the limiting attacks on Simon and Speck have been observed to be differential and linear attacks, it is important to understand the linear and differential properties of the algorithms. Fortunately, this has been a focus of the academic research, and it was an area we paid considerable attention to in our design effort.
>
> The design team used standard techniques (Matsui's algorithm, SAT/SMT solvers) to determine optimal differential and linear paths for Simon and Speck. We agree with the results obtained by outside researchers.

Reading this, the expectation was that the design team would explain in detail the methods used to bound the length of differential and linear paths[3] and release their tools so that the results they obtained can be reproduced. Instead, they proceeded to describe academic works, sometimes veiling published results as original work by the design team.

[2] We remind the reader that the algorithms were published in June 2013, i.e., 4 years prior.

[3] The designers use the term "path" in place of the more common terms "characteristic" and "trail" and we will follow suit.

Moreover, it is a known secret that differential and linear paths do not give the full picture due to the "multipath effect".[4] The designers also acknowledge this and wrote for Simon:

> As has been noted by various authors [3, 4, 19, 138, 490, 523], Simon has a strong multipath effect, largely because of the simplicity of its round function ... We might very conservatively estimate that the number of rounds admitting detectable linear correlations (12, 16, 20, 29, and 37) increases by 50% or so, in the worst case.

How this number (50%) was obtained remains unknown.

Similarly, the multipath effect for differences in Speck is simply stated without explanation:

> For Speck, there is also a slight multipath effect for differences and so an additional round or two can be gained, as noted by Song et al. [537]

and the multipath effect for linear approximation is not quantified at all:

> The linear paths tend to exhibit a stronger multipath effect, but the best linear attacks for Speck are still worse in every case than the best differential attacks.

To understand how the design team determined these numbers is crucial not only for understanding the security of Simon and Speck, but if properly done it can help in improving the security of other algorithms.

4.3.2 Choice of the Number of Rounds

A major source of contention within ISO was the lack of any information on how the round numbers were chosen. Table 4.1 gives the number of rounds for the various variants of Simon. We can see from this table that there does not seem to be any rule for choosing the number of rounds (or "stepping", as it is called in [66]). For example, moving from Simon48 with $m = 3$ to $m = 4$ does not change the number of rounds, while the same change adds two more rounds for Simon64 and Simon96, and 3 more rounds for Simon128.

The only concrete claim in [66] is about the security margins.[5] The designers say:

> Thus, the design team set the stepping with the aim of having security margins comparable to those of existing and trusted algorithms, like AES-128. After 4 years of concerted effort by academic researchers, the various variants of Simon and Speck retain a margin averaging around 30%, and in every case over 25%. The design team's analysis when making stepping decisions was consistent with these numbers.

[4] The term "multipath effect" used by the designers is also known as the "clustering effect", "differential effect", or "linear hull effect".

[5] The security margin is the difference between the number of rounds that can be attacked and the actual number of rounds.

In an attempt to determine the real security margins, ISO experts tried to piece together all the claims made by the designers. First, we looked at the best paths given in [66]:

> The design team determined that the single path probabilities (and linear correlations) dip below $2^{-\text{block size}}$ for 12, 16, 20, 29, and 37 rounds for Simon 32, 48, 64, 96, and 128, respectively.

Then, for the multipath effect they argue:

> Simon has a strong multipath effect, largely because of the simplicity of its round function ... We might very conservatively estimate that the number of rounds admitting detectable linear correlations (12, 16, 20, 29, and 37) increases by 50% or so, in the worst case.

That an additional round on each side of a Feistel network can be attacked is acknowledged:

> And then first/last round attack ideas must be factored in.

Pasting all these pieces of information together reveals that except for the case of Simon32/64, which retains a security margin of 37.5%, the remaining security margins for all other variants are below 30%, ranging between 12.5–27.8% with numbers that tend to decrease for the larger block sizes. The exact figures can be found in Table 4.3.

For Speck, the so-called design rationale focuses on differential cryptanalysis:

> the stepping was based on the best differential paths, which tend to be stronger than the best linear paths. See [223]. The single difference path probabilities dip below $2^{-\text{block size}}$ for 10, 12, 16, 18, and 21 rounds for Speck 32, 48, 64, 96, and 128, respectively.

The multipath effect is not quantified and the report only reads:

> For Speck, there is also a slight multipath effect for differences and so an additional round or two can be gained, as noted by Song et al. [537].

Table 4.3 Remaining security margins for Simon

Variant	Number of rounds	Longest path	150%	150% + first/last round trick	Remaining security margin (rounds)
32/64	32	12	18	20	37.5% (12)
48/72	36	16	24	26	27.8% (10)
48/96	36	16	24	26	27.8% (10)
64/96	42	20	30	32	23.8% (10)
64/144	44	20	30	32	27.3% (12)
96/96	52	29	43.5	45.5	12.5% (6.5)
96/144	54	29	43.5	45.5	15.7% (8.5)
128/128	68	37	55.5	57.5	15.4% (10.5)
128/192	69	37	55.5	57.5	16.7% (11.5)
128/256	72	37	55.5	57.5	20.1% (14.5)

A method which uses the key recovery procedure to attack additional rounds is mentioned:

> Dinur [183] shows that an r-round differential distinguisher yields at least an $(r+m)$-round attack, where m is the number of words of key.

For linear cryptanalysis the designers make a vague statement:

> The best linear paths for Speck are notably weaker than the best difference paths, with squared correlations dropping below $2^{-\text{block size}}$ in fewer rounds than is necessary for the difference path probabilities. This agrees with what was found (through non-exhaustive searches) in [223].

Then they cite again someone else's work, but only for Speck32, Speck48, and Speck64:

> In [377], it's proven that for Speck 32, Speck 48, and Speck 64 the squared correlations fall below $2^{-\text{block size}}$ in 10, 11, and 14 rounds, respectively.

The multipath effect is again mentioned, but not in a meaningful way:

> The linear paths tend to exhibit a stronger multipath effect, but the best linear attacks for Speck are still worse in every case than the best differential attacks.

In the case of Speck, not only does no variant retain a security margin of 30% as is argued in [66], but also the largest security margin is 18.2% for Speck32/64. The exact figures can be found in Table 4.4.

We stress that the estimation of the remaining security margin given here is very generous. It assumes that no path longer than those already found exists (which the designers refused to confirm), that the first/last round trick can indeed only be applied to a single round on each side, and that unlike Speck, key recovery attacks against Simon cannot extend beyond the statistical property being used.

Table 4.4 Remaining security margins for Speck

Variant	Number of rounds	Longest path	Multipath effect (+2)	Multipath effect + m	Multipath effect + m + first/last round trick	Remaining security margin (rounds)
32/64	22	10	12	16	18	18.2% (4)
48/72	22	12	14	17	19	13.6% (3)
48/96	23	12	14	18	20	13% (3)
64/96	26	16	18	21	23	11.5% (3)
64/144	27	16	18	22	24	11.1% (3)
96/96	28	18	20	22	24	14.3% (4)
96/144	29	18	20	23	25	13.8% (4)
128/128	32	21	23	25	27	15.6% (5)
128/192	33	21	23	26	28	15.2% (5)
128/256	34	21	23	27	29	14.7% (5)

Even under these generous assumptions the security margins seem slightly on the unsafe side. Surprisingly, it appears that the security margin decreases with the block size and that for about half of the variants the security margin is below (sometimes well below) the claimed 25%. In particular, by the time this so-called design rationale was finally released, only the 128-bit variants of Simon and Speck were considered for standardization in ISO with their extremely small security margins.

After facing these comments, the designers updated [66] and changed the 50% figure for the multipath effect to 25% adding a footnote which reads:

> The original version of this paper said 50% here, but noted that this was "very conservative." This led to confusion by some, who interpreted 50% as an exact value, rather than the very conservative upper bound we intended it to be. This is supported by the literature (see, e.g., [138]) and by our internal analysis. Indeed 50% is a significant overestimate; 25% appears to be a more accurate estimate. We apologize for the lack of clarity here, and note that even if future advances increased the 25–50% Simon would still be secure.

In fact, this footnote is liberal with the facts. In a private correspondence between the design team and one of the ISO experts, the former writes:

> Interestingly, for 18 rounds, it appears that there *is* likely a distinguisher. However, it's not a slam dunk ... However, I think the existence of such a distinguisher could likely be supported by analytic arguments...

4.3.3 Misquoting Existing Work

Following an extended discussion about differential and linear paths the designers proceed to briefly discuss other, less notable attacks. When reading this section with an expert's eye it becomes clear that some of the claims are outdated, either intentionally or unintentionally. One claim stands out in particular in the paragraph discussing slide and rotational attacks. The designers write:

> Both Simon and Speck employ round counters to block slide and rotational properties ...
>
> We note that, as with many block ciphers, the counters are essential elements of the designs; without them there are rotational attacks. In fact a very early analysis paper described a rotational attack on Speck, but it only worked because the authors of that paper mistakenly omitted the counter (see [6] (20130909 version)). Also see [28].

The uninformed reader may understand this paragraph to mean that rotational attacks are avoided by injecting round constants into the state and that this approach is supported by Ashur and Liu [28]. While adding round constants is indeed a common countermeasure against rotational attacks, the aforementioned [28] actually presents a novel method for building rotational distinguishers despite the algorithm's use of round constants. To drive the point home [28] exemplified the new method by building a rotational property for Speck. It is therefore not surprising that [376], a follow-up work to [28] used this method to build the longest distinguisher against certain variants of Speck using rotational cryptanalysis (surpassing

differential and linear cryptanalysis which were deemed by the designers to be the limiting attacks).

4.4 The ISO/IEC JTC 1 Standardization Process

The work in ISO/IEC JTC 1 is done at two levels: expert- and country-level. Officially, members of JTC 1 are countries, and, more particularly, national standardization bodies (NBs) within these countries. In various stages of the standardization process (e.g., amending an existing standard, canceling a project, approval of Committee Drafts (CD), etc.) NBs are requested to vote on certain questions via a procedure called a *formal ballot*.

Meetings are held every 6 months, each time in a different country. The national bodies send national *experts* to the meetings to discuss the ballots' results, which happen between these meetings, and resolve comments and disagreements.

The rules for how standards are developed in JTC 1 are governed by the ISO/IEC Directives Parts 1–2 [295, 296], which are publicly available documents. In particular, [295, Sec. 2] (Development of International Standards) outlines the various steps a project should follow before being accepted as a part of an international standard.

Being international and market-driven in nature, the work of ISO/IEC JTC 1 focuses around the concept of *consensus*. The importance of reaching consensus is described in [295, Foreword]:

> Consensus, which requires the resolution of substantial objections, is an essential procedural principle and a necessary condition for the preparation of International Standards that will be accepted and widely used. Although it is necessary for the technical work to progress speedily, sufficient time is required before the approval stage for the discussion, negotiation and resolution of significant technical disagreements.

A more refined procedure for determining whether consensus has been reached appears in [295, Sect. 2.5.6], which we mention further below.

When developing a new standard or amending an existing one, an editor and possible co-editor(s) are assigned to the project. The role of the editor is to manage the comments received from the various stakeholders, resolve them, and integrate the changes into the draft text. Target dates are also set for each project. A project that does not meet its target dates is automatically canceled, although extensions are possible.

For a better understanding of the standardization of Simon and Speck, and its resulting cancellation, we now briefly explain some of the important stages of the process.

Study Period

The standardization process for a new algorithm starts with a Study Period (SP). In this, a Call for Contributions (CfC) is drafted and sent to stakeholders. The stakeholders are requested to provide their views on the new proposal. The CfC

usually includes questions about the necessity for the new proposal, its security, possible use cases, how it compares to algorithms in existing standards, etc.

The decision to initiate a new working item as a result of an SP is made by the experts participating in the following meeting, and approved by NB ballot.

Working Draft (WD)
Once it has been decided to initiate a project, a working draft is circulated among the experts associated with the Working Group (WG) in charge of the project. The role of the project editor is to receive, resolve, and integrate comments from the experts to build consensus. A Working Draft (WD) usually undergoes several revisions until the experts agree that it is ready to progress to the Committee Stage as a Committee Draft (CD).

Committee Stage (PDAM, Proposed Draft Amendment)
The committee stage is the principal stage at which comments from NBs are taken into consideration. Once the Working Group experts agree that a draft proposal is mature enough to progress to the Committee Stage, a ballot is sent to all NBs which are requested to vote to approve this draft. While NBs are obliged to vote, the internal process through which the NBs vote is decided is governed by its own internal working procedures. When an NB wishes to vote to reject a proposal, they must also provide justification. Many of the national bodies do not have the required expertise to evaluate all proposals they receive and they either abstain or automatically approve proposals, by default.

The goal of the Committee Stage is to reach consensus among the national bodies involved. The definition of consensus is given in [217] and [295, Sect. 2.5.6]:

> Consensus: General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments.
>
> NOTE: Consensus need not imply unanimity. . . . in case of doubt concerning consensus, approval by a two-thirds majority . . . may be deemed to be sufficient for the committee draft to be accepted for registration as an enquiry draft; however, every attempt shall be made to resolve negative votes.

Further Stages
A consensual proposal that has been approved in the committee stage goes through more stages until its final publication. Since Simon and Speck, the subjects of this chapter, did not make it past the committee stage we do not explain the further stages here, and refer the interested reader to [295, Sec. 2].

4.5 The Standardization Process of Simon and Speck in ISO/IEC 29192-2

ISO/IEC 29192 [218] is a standard managed by the Joint Technical Committee (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard is managed by

Subcommittee 27 (SC 27) which is responsible for *information and IT security*. Within SC 27, the standard is edited by Working Group 2 (SC 27/WG 2) which is responsible for *cryptography and security mechanisms*. ISO/IEC 29192 itself is a multipart standard dealing with *lightweight cryptography* and Part 2 deals with *Block ciphers*.

The standardization process of Simon and Speck was improper from the outset. It involved premature submission of the algorithms, assignment of the Simon and Speck designers as the project editors, using erroneous procedures to promote the algorithms, refusal to respond to technical questions and a generally adversarial approach towards the process. For brevity, we describe in the sequel the timeline of the standardization process starting from the initial study period and until the project was finally canceled.

Mexico City, Mexico (October 2014)
The idea to include Simon and Speck as part of ISO/IEC 29192-2 was formally launched in the WG 2. A Study Period (SP) was initiated in November 2014 and there was a Call for Contributions for a period of 18 weeks.

Kuching, Malaysia (April 2015)
The responses in the study period were registered. Responses from 4 NBs were received: two supporting the standardization (Russia and the US) and two objecting (Norway and Germany). A presentation was given by Doug Shors discussing the comments submitted by the NBs.[6]

The meeting report indicates that a discussion was held about some of the submitted comments, resulting in a compromise which extended the study period by 6 months to request further input on the algorithms' security, while also allowing a Preliminary Working Draft (PWD) to be circulated in parallel. Interestingly, the most critical question in the Study Period, Question 1, "Should SIMON and SPECK be included in ISO/IEC 29192-2?" is not addressed in the meeting report despite negative responses from some NBs. It is this meeting summary that would later be used by the editors to argue that a decision to include Simon and Speck in ISO/IEC 29192-2 had already been made and could not be contested anymore.

The new Call for Contributions and the Preliminary Working Draft were circulated in May 2015 and June 2015, respectively. At this point, the new CfC no longer included any question of whether Simon and Speck should be standardized, suggesting that the NSA had already decided by then to act in a way that was adversarial to the process.

Jaipur, India (October 2015)
The circulation of the extended CfC following the previous meeting resulted in several experts' comments. About half of the experts commented that the security

[6]Doug Shors and Louis Wingers are two NSA employees listed as part of Simon and Speck's design team. They were assigned as co-rapporteurs for this study period, and later as co-editors of the project.

of Simon and Speck was not yet fully understood, and additional information, preferably in the form of a design rationale, was requested.[7]

In parallel, two responses to the Preliminary Working Draft, editorial in nature, were received. Both the comments made in the study period and the ones on the Preliminary Working Draft were discussed in a presentation by Louis Wingers. In this presentation, Wingers argued that providing a design rationale was not the designer's job, and that cryptanalysis of both algorithms had stabilized such that no new results were expected to be published.[8]

Not mentioned in the meeting summary is a discussion that was held about past involvement of the NSA in sabotaging cryptographic standards, e.g., Dual-EC. One of the NSA experts, Debby Wallner, who was also involved in the standardization of Dual-EC, referred to it as the "elephant-in-the-room" and claimed that they had apologized for it and that it was time to move on.[9]

Also not reflected in the summary is a request by Wallner to have a country-level vote during the meeting in order to decide how to proceed with the project. This vote, which has no grounds in the ISO directives, had to be later ratified using the correct procedure. By then, the meeting summary had already noted that the study period should be terminated and that a first Working Draft should be circulated.

Tampa, Florida, USA (April 2016)

Simon and Speck's Working Draft (WD) was circulated on November 2015 with a commenting period of 17 weeks (until March 2016). Aside from editorial remarks, the comments received make it clear that many experts did not trust the security of these algorithms. Another concern raised by experts was that many experts disagreed with the editors' decision to leave variants of Simon and Speck with a 48-bit block size in the draft.

In their Disposition Of Comments (DoC), the editors refused to address the security concerns raised by the experts, virtually marginalizing what seems to be the majority's opinion; quoting from the first paragraph of their response:

> The decision to initiate this Amendment which includes SIMON and SPECK has already been made.

Reading the comments about small block sizes, the editors decided to shift the discussion outside of their own project, and started yet another Study Period (SP) dealing with the more general question of small block sizes.

In conclusion, the meeting report writes:

> The session ended by trying to determine how to move forward. To do this, Debby Wallner (US) requested that a straw poll be taken to decide if the proposed Amendment should move

[7] This would be a recurring theme in the standardization of Simon and Speck.

[8] This is yet another recurring theme in the standardization of Simon and Speck. This claim was made by the NSA in each and every meeting, and was always defeated by the time of the next meeting.

[9] Since the discussion about Dual-EC is not reflected in the meeting summary, it is reproduced here from memory.

> to second working draft or to the ballot stage. All experts in attendance were asked and the result was 16 to 8 in favor of a second working draft with 8 abstentions.

Such numbers, especially in a preliminary stage, show that the algorithms did not enjoy the wide support required for standardization. Nevertheless, since it was the editors' responsibility to implement the decisions, they concluded the meeting, writing:

> The Editor will now draft a new Call for Contributions which will make three requests. First, a request to outline security concerns with the use of a 48-bit block cipher. Secondly, a request for potential use cases for a 48-bit block cipher. Finally, a request for any updates on the ongoing security evaluation of SIMON and SPECK.

Abu Dhabi, UAE (October 2016)
Indeed, another Working Draft was circulated on June 2016 with a commenting period of 15 weeks (until September 2016). Surprisingly, the Working Draft only included questions about the block size, and about new cryptanalytic results, completely ignoring the mistrust expressed by the majority of experts. As a result, comments about this working draft were limited to the questions asked and referred only to the block size.

In their Disposition of Comments, the editors resolved to remove the 48-bit variants of Simon and Speck and leave the other block sizes.[10] They also resolved all editorial comments and declared that a consensus has been reached and that the draft was ready to progress to Committee Stage.

Hamilton, New Zealand (April 2017)
Simon and Speck's 1st PDAM was circulated on December 2016 requesting that votes and comments be sent until February 2017. The result of this ballot showed that 15 NBs voted to approve the proposal (some with comments), 8 voted to disapprove, and 26 abstained. This result showed not only that the algorithms do not enjoy consensus, but also even the 66% minimal threshold was not met.

Many of the comments from the National Bodies listed the absence of a design rationale as a factor in their disapproving vote. Other comments also mentioned that 64-bit block ciphers were inherently insecure against generic attacks.[11] In their preliminary Disposition of Comment the editors announced that they would provide a design rationale for the algorithms:

> The editors will provide documentation that discusses the design rationale and the design team's security analysis for SIMON and SPECK.

[10] Since the efficiency of the two algorithms, which was its main selling point, was always presented with respect to the smaller variants of the algorithms, it is interesting how the smaller variants have been slowly phased out of the proposed standard, leaving only the larger variants whose efficiency was never thoroughly discussed and that do not fare as well as the alternatives.

[11] The Sweet32 attack [86] was published around this time and was a factor in many of the decisions of the NBs.

but the editors refused to address the comments about small block sizes. Following a heated discussion in the meeting itself, they announced that they would remove all variants of Simon and Speck with block size smaller than 128-bits.

Berlin, Germany (October 2017)
The so-called design rationale was circulated together with the 2nd PDAM asking again the national bodies to approve or disapprove this project within 8 weeks. This time, the results were that 15 countries voted to approve the draft (some with comments), and 7 voted to disapprove. This vote, while still not consensual, at least met the 66% threshold allowing the secretariat to deem such vote consensus.

The so-called design rationale and the problems that arise from it were analyzed in Sect. 4.3 and most of these comments were also submitted as part of the National Bodies (NBs) justifications for disapproval. The editors refused to address these comments, and provided the following standard answer to comments from NBs:

> The editors regret that [Country X] feels that there is insufficient design criteria provided for SIMON and SPECK in order to determine their inclusion in ISO/IEC 29192-2. . . . No further design rationale will be provided by the editors for SIMON and SPECK. The editors stand behind their position that all the documents previously referenced as a part of this Disposition of Comments do indeed provide sufficient information to determine that SIMON and SPECK are indeed secure.

A particular focus was put in this meeting on how the number of rounds was chosen for the algorithms. The NSA editors argued that Tables 4.3 and 4.4 are a misunderstanding and that

> Any native English speaker would immediately understand what we were trying to say in the design rationale.

When asked to elaborate about this decision for the sake of the non-native English speakers in the room, they simply refused. Furthermore, the editors also refused to answer the following two questions posed to them:

- When releasing the algorithms in 2013, was the NSA aware of all attacks that were later published by the academic community against these algorithms?
- Is the NSA aware of additional attacks, beyond those already discovered and published by the academic community?

Their refusal to answer these questions, together with the insufficient quality of the design rationale, was enough to demonstrate that "sustained opposition to substantial issues" still existed, and it was decided that a 3rd PDAM should be circulated.

Wuhan, China (April 2018)
The 3rd PDAM was circulated on December 2017, again asking for the support of national bodies within 8 weeks (until February 2018). This time, 14 countries

voted to approve the draft (some with comments), and 8 voted to disapprove. The Disposition of Comments was not distributed prior to the meeting and was made available to participants only in the meeting itself. The project editors could not attend the meeting in-person and the editing session was performed via Skype. At this point, it was made clear that the editors had given up on reaching consensus. They refused to address the concerns raised by the NBs, and simply said that they requested that a 4th PDAM be circulated. In response, some of the experts suggested that since it is clear that a consensus cannot be reached due to the refusal to provide further information, the project should be canceled.

Following a discussion about the proper procedure to make this decision, the WG2 conveners decided to hold an internal vote. Each country participating in the meeting would cast a single vote for one of the following options: (1) cancel the project; (2) proceed to a 4th PDAM; and (3) abstain. Of the 16 countries represented in the room, 8 voted to cancel the project, 4 voted to move to a 4th PDAM, and 4 abstained. This decision was later ratified by SC27, the parent committee to WG2.

The justification for cancellation reads:

> Working Group 2 (WG 2) feels that both algorithms included in the amendment are not properly motivated and their security properties are not sufficiently understood. An attempt was made by the designers to publish a design rational (ePrint 2017/560) which was not enough to convince WG 2 experts. Requests to disclose additional information about the way the algorithms were designed were refused by the designers.
>
> It appears that a stalemate has been reached where the amendment cannot reach the required majority of 66% to move from PDAM to DAM stage. This issue seems to already reflect badly on ISO's reputation in what media attention it receives. It also has an adverse effect on the collaborative nature of the work within ISO which seems to polarize around this and spill over onto other projects. Therefore, WG 2 experts believe that it is best to cancel the project and not standardize these algorithms.
>
> WG 2 wishes to convey that not including the algorithms in ISO/IEC JTC 1/SC 27 standards is not a statement about the security or the quality of the algorithms nor about the work done by the designers nor the editors. Since the decision to move forward from a PDAM stage requires consensus decision (even if not unanimity) it simply means that given the available information and the opposing opinions about the security of the algorithms they do not enjoy the level of confidence required for inclusion in ISO/IEC JTC 1/SC 27 standards.