ISO/IEC JTC 1/SC 27/WG 2
Cryptography and security mechanisms
Convenorship: JISC (Japan)

Document type:	Meeting Report
Title:	Meeting Report for the Discussion on Kuznyechik and Streebog
Status:	
Date of document:	2019-04-16
Source:	Session Chair (Hirotaka Yoshida), Session Co-chair (Jonathan Hammell)
Expected action:	INFO
No. of pages:	1 + 6
Email of convenor:	t-chika@ipa.go.jp
Committee URL:	https://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2

Meeting Report for the Discussion on Kuznyechik and Streebog

The session was chaired by Hirotaka Yoshida (JP) and co-chaired by Jonathan Hammell (CA). Each National Body (NB) that contributed statements on this issue summarized their contribution.

Stefan Kölbl (DK) said that there are some academic papers that describe structure in the S-Box. The contributions at the time of proposal for standardization did not present this structure. DK would like an explanation of clarification from RU (as proposers of these algorithms). At FSE, the author of the academic paper said that the probability of this structure is low.

Stephan Krenn (AT) said that he had not much to add to the DK comments. AT experts found the evidence surprising, and would like an explanation of why it was not disclosed. If it can be shown that it can happen by chance with sufficiently high probability, then they would like time to analyze if these properties lead to attacks.

Liqun Chen (GB) is not the expert for this topic, but the UK experts believe that it is vital for the credibility of the group that before the algorithms are adopted as a standard, that the group be provided an explanation of the structure of the S-box. They also request time to consider whether the explanation provided is adequate. Would like to investigate the possibility of removing Streebog if the explanation is deemed not to be sufficient.

Derek Atkins (US) summarized that he agrees when the points raised by other countries and would like more study on algorithm and that it is not ready to be standardized at this point.

Pascal Paillier (FR) summarized that FR is concerned about the issue in the S-box. They want the issue to be discussed to know what happened. Pointed out that the algorithms are in different stages (Streebog is already standardized). Also noted that SM4 amendment was merged with Kuznyechik and how we address Kuznyechik should not affect the standardization of SM4. Consideration of inclusion and deletion, but the working group does not have a procedure for "quarantine". FR believes that transparency is essential and the credibility of WG2 is at stake. Perhaps we should make it clear (like on a webpage) that the issue is under study, so that observers outside of ISO are aware we are addressing it.

Tobias Mikolasch (DE) said everything has been addressed by the other NB contributions. We need more clarification before we move ahead with the standardization process.

Hiro asked if any other countries had comment before giving the floor to RU. Orr Dunkleman (IL) supports the comments of the previous contributions. Gaetan Pradel (LU) supports the FR position. Kan Yasuda (JP) gave the history of the standardization. In Hamilton, NZ (2017) we discussed the 1st working draft. There was an empty sub-clause in the WD and JP made a comment that it should be removed. But the explanation from the editor that this sub-clause was to describe the S-box, but the editor claimed that the PDF conversion removed this text. In Wuhan, the S-box appeared in this section. The editor said it was the same S-box. JP asked how it was generated, and the response was that it was chosen at random. Now JP asks how it was chosen by random such that it satisfies these properties. Stephan Krenn noted that there was a statement after Wuhan that it was generated from a

pseudorandom search and not chosen with specific properties. Given this, it is surprising that the discovered properties are present. Gerard Vidal (ES) supports the FR position.

Hiro explained that he is neutral, but there may be procedural issues with those proposed by FR.

Vasily Shishkin (RU) responded on behalf of RU and the design team for the algorithms. He thanked Léo Perrin and other scientists for their interest in the algorithms. The results do not contain any attack or weakness. Léo's paper includes this same statement. RU believes that for almost any S-box we can find a partition in the structure. Any partition is valuable because it provides implementation flexibility. A partition is of concern only if it leads to an attack. RU did not know of this construction and that they have never hidden their design construction. At the time, it was not common to provide the initial values for the search algorithm, so they did not provide it.

Vasily provided some personal comments. In response to Kan's notes, the algorithms were standardized in the Russian Federation and so it would have been impossible to change P. These algorithms are standardized for the protection of up to classified information in Russia, not just sensitive information. It would be "dumb" to put a vulnerability in algorithms they are using to protect their own sensitive information. He believes that it would be a significant research breakthrough to demonstrate how to use partitions in the S-box to put a backdoor in an encryption or hash algorithm. At Lightweight Crypto Day hosted at Bar Ilan University, an attack was announced on 5 rounds of AES with complexity 2^{16}. Is it a concern? Which concern (re. AES or Kuznyechik) is greater? Furthermore, SHA-1 is broken. We have a collision. Yet, we only have a warning "don't use in certain situations". Therefore, we should be more concerned that we have broken algorithms in our standards than properties that do not lead to attacks.

Stephan Krenn repeated that experts are not claiming that there is an intentional backdoor in the algorithms, but rather would like more time to study the property. The quote from Léo's paper cited by Vasily ended with "but we question the design choice." Stephan requests a six-month study period to concern whether the recent research is a risk or not.

Orr Dunkleman, as coauthor of results on 5 round AES, said the 5 round attack does not mean that it extends even to 6 rounds of AES. He also does not think a backdoor was put into the design. However, if you have certain specific properties in an S-box, they can be use to generate attacks. Additionally, in response to Vasily's claim about a breakthrough would be necessary to construct a backdoor, he pointed out that there are much earlier works on how to construct backdoors in symmetric algorithms. On the TKLog structure, Orr would like to understand a) its impact on security and b) how likely such properties will happen by chance.

Tobias Mikolasch commented on Vasily's point about the use of the S-box in government use. He thinks that more information on how it was designed can be provided. Vasily responded that it was already provide prior to the last meeting.

Tomer Ashur (BE) said that Léo's paper is remarkable, yet he has some reservations about the paper's claims about the probability since that this group may know that the probability could be higher. Since this cipher is used in Russia, the research should be of interest to RU government. Therefore, they should support more investigation of this research. Tomer said that he thinks we should wait for standardization.

Vasily responded that previous publications of Kuznyechik and Streebog inspired work by scientists in RU and that discovered properties in the S-box. Had they known these properties, they would have changed the S-box. Vasily confirmed that he believes the S-box is sub-optimal.

Tanja Lange disputed the claim that the transparency about the generation of S-boxes was not present at the time of the design of Kuznyechik and Streebog. For example, during the AES competition, before the design of Kuznyechik. She asked for RU scientists to try to regenerate the S-box design procedure. She also said that the argument that government use precludes backdoors is not valid since the US had recommended Dual EC DRBG for government use.

Tomer Ashur said there is a misunderstanding. The note from RU said that they disqualified S-boxes based on certain properties. He asked for the list of properties that were used for disqualifying S-boxes. Stephan Krenn said there were five properties listed in the note, but more accurate bounds on these properties would be necessary for replication. This could be done offline. Tanja said that code could be provided.

Stefan Kölbl and Tanja Lange asked if the S-box was chosen at random, then was that S-box discarded to choose the next one or was it tweaked from one choice to the next. Vasily responded that the S-boxes were chosen independently at random. Tanja asked how they sampled to choose the S-box. Vasily said it was chosen one byte at a time and the properties such as permutation and fixed points was checked after all the samples were made. They stopped searching for better S-box when they were "exhausted". Orr Dunkleman asked how much computation effort was put into the generation of the S-box. Vasily said he can provide an estimation, but not right now.

Hiro asked that we have to address the two issues (10118-3 and 18033-3) to take some action. We have to make a statement to defend our credibility in response to the IACR research. Grigory Marshalko (RU) asked why we need to make a statement about this one and not about other standardized algorithms that are weak (like SHA-1) and mechanisms that have no clear origin (e.g. MASH and MQ DRBG). Algorithms like SHA-3 and SHAKE have "clear distinguishers". No attack on Kuznyechik or Streebog is demonstrated in research. When did the rules change? Maybe we should reassess all the algorithms or start a Study Period on backdoors?

Hiro said he thinks that we should take immediate action to address 10118-3. But he suggested moving on to SD5 and reopen this issue tomorrow. An RU expert asked if "concern" is a sufficient reason to start the process to reconsider standardized algorithms. If there are no rules in a SD, then it sets a dangerous precedent. Stephan Krenn said that he would support a study period on reconsidering standardized algorithms. Stanislav Smyshlyaev (RU) suggested to postpone the standardization of Kuznyechik and start a six-month SP with explicit questions:

1. Do you have any real attacks on Kuznyechik?
2. Do you have any real attacks on Streebog?

Derek Atkins agreed that this might be a good approach and US would appreciate this time to study.

Discussion from the Second WG2 Session

Jonathan Hammell (CA) summarized three actions that were proposed in the session yesterday. No action is also an option.

1. Make a public statement, such as on the ISO website, that we are studying the results published on Kuznyechik and Streebog
2. Start a six-month SP with two questions
   a) Are you aware of any attack on Kuznyechik?
   b) Are you aware of any attacks on Streebog?
3. Start a six-month SP investigating the provenance of all algorithms in WG2 standards.

Finally, we need to decided on how to proceed with the standardization of SM4.

Hiro talked with Toshio and there are three standards under consideration
1. 10118-3 is already published. This is the highest priority.
2. 18033-3 is an ongoing project to standardize Kuznyechik and SM4. Project will be frozen, causing a problem for the convenor. Though the project is not at risk of cancellation.
3. 9797-2 is already published with numerical examples using Streebog as a hash function in a MAC.

Hiro said that we are here to find some compromize. Tomer Ashur (BE) pointed out that there should be no concern with delaying 18033-3 for six months. Limin Liu (CN) agreed with doing a six-month study period and is okay with a six-month delay for SM4, but longer would be of concern. Tomer said that in the unlikely event that we with to delay Kuznyechik longer, then it may be theoretically possible to separate the two proposals. Limin wanted to have a plan for the possible separation. Toshio said he had asked Kristina and she said it is an editorial issue that is possible. But Toshio suggested that there is an ISO procedural concerns with delaying the circulation of FDIS for 6 months. Toshio has the proposed FDIS text, but it has not been sent to ITTF. Pascal Paillier (FR) asked if there was not a process to freeze a process in the Working Group. Walter Fumy (DE) said that the only target date for ISO is the DIS deadline and that it is possible to ask for an extension from ISO for up to six months.

Hiro asked if we all agree on a six month study period. Daniel Bernstein said that he believed we all agree with a study period, but he pointed out that we also need to ask about the probability of having such properties in the S-box as requested by many of the NB contributions.

Hiro asked for a break to confer with Toshio and relevant people. During the break, experts from RU and other countries worked on putting together questions for the study period. Toshio explained the limits in ISO's calendar for this project:
- June 13, 2020 is limit date for publication of the IS
- FDIS text must be sent within 2019, then ITTF will have 6 months to do FDIS ballot, implement comments and publish.

Consequently, we must agree on the text at the Paris meeting.

Vasily Shishkin displayed the proposed text for the Study Period.

Title: *Study Period on new results concerning Streebog and Kuznyechik S-box*

1. Do you have any information about existence of attack on Kuznyechik or Streebog more effective than generic ones? If yes, please provide corresponding information.
2. Can you quantify the probability of obtaining the TKLog structure (see ePrint 2019/092) for the S-box? Please specify your generation method for the S-box.
3. Can you quantify the probability of obtaining any other S-box structure? Please specify your generation method for the S-box.
4. Do you have any information about methods for obtaining any structure for random permutation?

Orr Dunkleman asked if someone has an answer to question 3, what does it mean for Kuznyechik and Streebog? Vasily said this is all for information purposes to determine more information about these S-box properties.

Stephan Krenn pointed out that the results of the study period will only be obtained two months prior to the Paris meeting, limiting the amount of time for NB consideration.

Daniel Bernstein said that questions 2-4 will possibly be a response to the results of Léo Perrin since the existing public opinion is that the S-box with TKLog structure cannot be found at random in a reasonable way.

Tobias Mikolasch (DE) asked what will happen in Paris if there is no input or answered "no" to questions 1-4.

Vasily stated that they are always willing to answer any question. Pascal Paillier asked if it is possible to replace the current S-box. Vasily responded that it is very difficult because these algorithms are standardized in Russia and other former Soviet countries. Stanislav Smyshlyaev (RU) added that the algorithms are in a lot of hardware and software. Another RU expert pointed out that following the publication of the results of Léo Perrin, Russian scientists discovered how to use the TKLog structure to obtain a better S-box.

In Paris, we will have two options for 18033-3 based on the results of the Study Period:
1. Continued with the FDIS text as submitted
2. CN rewrite FDIS text to remove the Kuznyechik and Kuznyechik text will become AMD1 again.

Toshio said he has no answer from ITTF on publishing AMD2 before AMD1.

Discussion from the Third WG2 Session

Everyone agreed for a WG 2 Study Period with the proposed title and text above. Vasily Shishkin (RU) and Stephan Krenn (AT) agreed to be rapporteurs.

Liqun Chen (GB) raised concerns over how to proceed at the Paris meeting depending on the results. Grigory Marshalko (RU) encouraged the group to leave this concern until the Paris meeting.

Toshio said he will delete the merged FDIS text from the Tel Aviv resolutions.

Resolution

The FDIS for 18033-3 will be delayed until the fall meeting in Paris. A six-month study period titled *Study Period on new results concerning Streebog and Kuznyechik S-box* will be started, with Vasily Shishkin (RU) and Stephan Krenn (AT) as rapporteurs, asking the following questions:

1. Do you have any information about existence of attack on Kuznyechik or Streebog more effective than generic ones? If yes, please provide corresponding information.
2. Can you quantify the probability of obtaining the TKLog structure (see ePrint 2019/092) for the S-box? Please specify your generation method for the S-box.
3. Can you quantify the probability of obtaining any other S-box structure? Please specify your generation method for the S-box.

4. Do you have any information about methods for obtaining any structure for random permutation?