From: Calik, Cagdas (IntlAssoc)
To: (b) (6) ; Sonmez Turan, Meltem (Fed)
Cc: McKay, Kerry A. (Fed); Bassham, Lawrence E. (Fed)
Subject: RE: family work
Date: Monday, August 5, 2019 10:42:39 AM

Spook was not presented, I'll do it.

Cagdas

From: Donghoon Chang (b) (6)
Sent: Monday, August 5, 2019 10:32 AM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Cc: McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Bassham, Lawrence E. (Fed) <lawrence.bassham@nist.gov>
Subject: Re: family work

Ok I will prepare for Quartet.

On Mon, Aug 5, 2019, 10:28 AM Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov> wrote:

> Donghoon,
>
> On Thursday, we will discuss the remaining algorithms.
>
> So far the assigned algorithms are Fountain (Meltem), Qameleon (Kerry) and Yarará and Coral (Craig).
>
> We need a speaker for Quartet, and we can briefly go over the results on Bleep64, CLAE, mixFeed, FlexAEAD, Sneik, Limdolen, Laem and SIV-tem-photon.
>
> Regards,
> Meltem
>
> **From:** Donghoon Chang (b) (6)
> **Sent:** Monday, August 5, 2019 10:21 AM
> **To:** Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
> **Subject:** Re: family work
>
> What will be the agenda for Thursday meeting?
>
> On Mon, Aug 5, 2019, 10:19 AM Donghoon Chang <(b) (6) wrote:
>
> > Ok I will read all the papers under security proofs.
> >
> > - Donghoon

On Mon, Aug 5, 2019, 10:16 AM Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov> wrote:

> Hi Donghoon,
>
> The meeting is in Thursday morning.
>
> Please select around 10 papers to review from the list (below) and let me know your selections **today**. Papers under security proofs will be a good choice. Larry and Cagdas will review implementation papers.
>
> Thanks,
> Meltem
>
> **Updates by submitters**
>
> - On the S-box in GAGE and InGAGE, Danilo Gligoroski
> - Fountain v1: A Lightweight Authenticated Cipher, Bin Zhang
> - Dumbo, Jumbo, and Delirium: Parallel Authenticated Encryption for the Lightweight Circus, Tim Beyne, Yu Long Chen, Christoph Dobraunig, and Bart Mennink
> - An Update on Qameleon, Roberto Avanzi, Subhadeep Banik, Andrey Bogdanov, Orr Dunkelman, Senyang Huang, and Francesco Regazzoni
> - Ascon v1.2 – Analysis of Security and Efficiency, Christoph Dobraunig, Maria Eichlseder, Florian Mendel and Martin Schläffer
> - Updates on Romulus, Remus and TGIF, Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin
>
> **Security Proofs**
>
> - Security Proof of mixFeed, Bishwajit Chakraborty and Mridul Nandi
> - Security Proof of ORANGE-Zest, Bishwajit Chakraborty and Mridul Nandi
> - ESTATE Authenticated Encryption Mode: Hardware Benchmarking and Security Analysis, Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas Lopez, Mridul Nandi, Yu Sasaki
> - Security Analysis of HyENA Authenticated Encryption Mode, Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri,Mridul Nandi
> - Security Proof of Beetle and SpoC, Bishwajit Chakraborty and Ashwin Jha and Mridul Nandi
> - On the Security of COMET Authenticated Encryption Scheme, Shay Gueron, Ashwin Jha, and Mridul Nandi
> - Security Proofs for Oribatida, Arghya Bhattacharjee, Eik List, Cuauhtemoc Mancillas López and Mridul Nandi

Cryptanalysis of the candidates

- Practical Forgery Attacks on Limdolen and HERN, Raghvendra Rohit and Guang Gong
- Slide Attack on CLX-128, Alexandre Mège
- A Practical Forgery Attack on Lilliput-AE, Orr Dunkelman, Nathan Keller, Eran Lambooij, and Yu Sasaki
- Cryptanalysis of Internal Keyed Permutation of FlexAEAD, Mostafizar Rahman, Dhiman Saha, Goutam Paul
- Forgery on Qameleon and SIV-TEM-PHOTON and SIV-Rijndael256, Nilanjan Datta, Ashwin Jha and Mridul Nandi
- Breaking REMUS and TGIF in the light of NIST Lightweight Cryptography Standardization Project, Nilanjan Datta, Ashwin Jha, Alexandre Mège and Mridul Nandi
- Distinguishers for Reduced Round Ascon, DryGASCON, and Shamash Permutations, Cihangir Tezcan

~~**Implementation of the candidates**~~

- ~~FELICS-AE: a framework to benchmark lightweight authenticated block ciphers, Kévin Le Gouguec~~
- ~~Hardware Implementations of NIST Lightweight Cryptographic Candidates: A First Look, Behnaz Rezvani and William Diehl~~
- ~~Benchmarking Software Implementations of 1st Round Candidates of the NIST LWC Project on Microcontrollers, Sebastian Renner, Enrico Pozzobon, Jurgen Mottok~~
- ~~LOTUS and LOCUS AEAD: Hardware Benchmarking and Security Analysis, Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas Lopez, Mridul Nandi, Yu Sasaki~~
- ~~Hardware Design and Analysis of the ACE and WAGE Ciphers, Mark D. Aagaard, Marat Sattarov, and Nusa Zidaric~~
- ~~A Comprehensive Framework for Fair and Efficient Benchmarking of Hardware Implementations of Lightweight Cryptography Jens-Peter Kaps, William Diehl, Michael Tempelmeier, Farnoud Farahmand, Ekawat Homsirikamol and Kris Gaj~~
- ~~Benchmarking and Optimizing AES for Lightweight Cryptography on ASICs, Jenny W. Yu and Mark D. Aagaard~~
- ~~FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms Luan Cardoso dos Santos, Johann Grobschadl, and Alex Biryukov~~
- ~~What the Fork: Implementation Aspects of a Forkcipher, Antoon Purnal, Elena Andreeva, Arnab Roy, and Damian Vizar~~
- ~~Implementation of three LWC Schemes in the WiFi 4-Way Handshake with Software Defined Radio, Yunjie Yi and Guang Gong~~

- ~~SNEIK Algorithms on Microcontrollers: AVR, ARMv7-M, and RISC-V (with Custom Instructions), Markku-Juhani O. Saarinen~~

Side channel attacks

- Analyzing the Leakage-Resistance of some Round 1 Candidatesof the NIST's Lightweight Crypto Standardization Process, Francois-Xavier Standaert
- Leakage Resilience of the ISAP Mode: A Vulgarized Summary, Christoph Dobraunig and Bart Mennink
- An Open-Source Platform for Evaluating Side-Channel Countermeasures in Hardware Implementations of Lightweight Authenticated Ciphers Abubakr Abdulgadir, William Diehl and Jens-Peter Kaps

On the need for LWC

- Cryptography in Industrial Embedded Systems: our experience of needs and constraints, Jean-Philippe Aumasson, Antony Vennard

~~Generic implementations~~

- ~~Will the Future Lightweight Standard be RISC-V Friendly? Gorkem Nisanci, Tolga Yalcin, Elif Bilge Kavun~~
- ~~Does gate count matter? Hardware efficiency of logic-minimization techniques for cryptographic primitives, Shashank Raghuraman and Leyla Nazhandali~~
- ~~Systematic Testing of Lightweight Cryptographic Implementations, Sydney Pugh, M S Raunak, D. Richard Kuhn, and Raghu Kacker~~

Out of scope

- Malfunctioning Inputs Detection Approach (Tool) based on Machine Learning [MIDT-SVM], Romil Rawat, Sachin Chirgaiya, Chandrapal Singh Dangi

From: Donghoon Chang (b) (6)
Sent: Monday, August 5, 2019 10:07 AM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Subject: family work

Dear Meltem,

When do we have meetings this week?
(b) (6)
What do I need to do for that?

- Donghoon