An overview of FAVPQC achievements

Kazuhiro Ogata (JAIST)

The 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC 2023)

November 21, 2023

Novotel Brisbane South Bank, Brisbane, Australia

Roadmap

- ICT for Resilient, Safe and Secure Society
- Quantum Computers as Security Threats
- How We Have Collaborated
- Formal Specification & Analysis of KEMs
- Tools Developed
- Formal Verification of PQ Protocols
- Events
- Some future directions

ICT for Resilient, Safe and Secure Society

Program Officer

Dr. Yuzuru Tanaka (Professor Emeritus, Hokkaido U.)

21 proposals submitted in 2020, and 6 accepted, funded by Japan Science and Technology Agency (JST) in collaboration with 10 funding agencies from 10 European countries in the framework of the EIG CONCERT-Japan under SICORP for 3 years (April 2021 – March 2024)

The EIG CONCERT-Japan is the continuation of FP7.

ICT for Resilient, Safe and Secure Society

One of 6 accepted proposals is

Formal Analysis of Verification of Post-Quantum Cryptographic Protocols (FAVPQC)

Santiago Escobar

(Spain)

Sedat Akleylek

(Turkey/Estonia)

Ayoub Otmani

(France)

Kazuhiro Ogata

(Japan)

ICT for Resilient, Safe and Secure Society

The funding agencies of FAVPQC are as follows:

- France: National Centre for Scientific Research (CNRS)
- Japan: Japan Science and Technology Agency (JST)
- Spain: Agencia Estatal de Investigación (AEI) - State Research Agency
- Turkey: The Scientific and Technological Research Council of Turkey (TUBITAK)

Quantum Computers as Security Threats

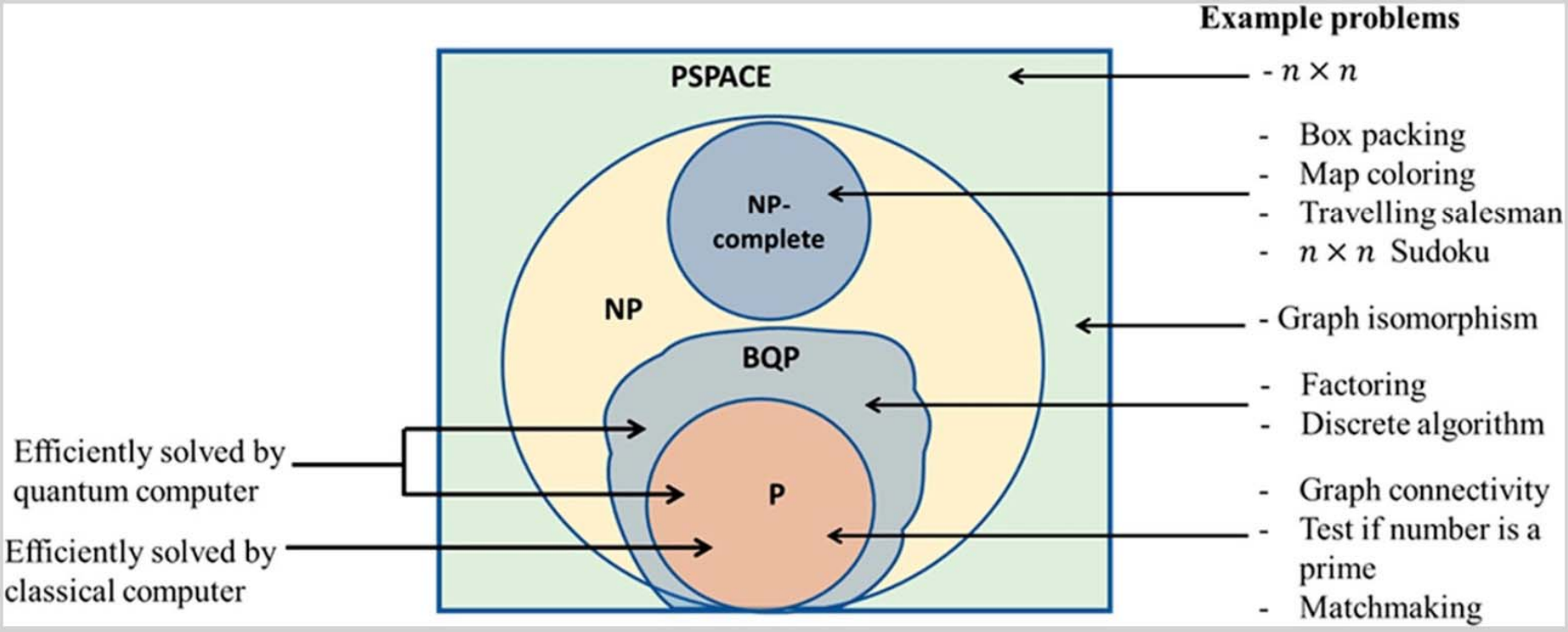
- An idea of quantum computers proposed by Faynman, etc. early-80's
- Google, etc. have been spending many resources (money, humans, etc.) toward implementation of large-scale quantum computers
- Shor invented the quantum algorithm that can efficiently solve integer factorization in 1994

Quantum Computers as Security Threats

- Public-key encryption schemes, such as RSA, currently used will become insecure and unsafe when large-scale quantum computers are available
- Cryptographic primitives, such as KEMs, resistant to quantum computers are actively studied (in the middle of selection of future standard ones by NIST)
- Development of technologies that can be used to guarantee that post-quantum cryptographic protocols are really secure and safe is an urgent research topic

Quantum Computers as Security Threats

Quantum computing supposes a threat to security



BQP stands for bounded-error quantum polynomial time

Quantum Computers as Security Threats

Quantum algorithms that can affect the current cryptographic primitives

- Shor’s algorithm
  - Integer factorization
- Grover's algorithm
  - Unstructured database search

How We Have Collaborated

Cryptographers


Sedat


Ayoub

Formal methods experts


Kazuhiro


Santiago

Introduction of promising
PQ cryptographic primitives

Development of PQ
cryptographic primitives, etc.

Development/modification
of support tools

Formal analysis & verification
of PQ protocols

Discussion of analysis/verification results

Tools & Techniques Used

- Maude – model checking facilities (LTL model checker & search command)
- Maude-NPA – backward narrowing-based search with many optimization techniques
- CafeOBJ – proof score-based interactive theorem proving
- CafeInMaude – World's 2nd implementation of CafeOBJ in Maude, equipped with a proof assistant (CiMPA) and a proof generator (CiMPG)

Formal Specification & Analysis of KEMs

D.D. Tran, K. Ogata, S. Escobar, S. Akleylek, A. Otmani: Kyber, Saber, and SK-MLWR Lattice-Based Key Encapsulation Mechanisms Model Checking with Maude, IET Information Security 2023: 9399887 (1-17), Hindwa (2023)

V. García, S. Escobar, K. Ogata: Modelling and verification of post-quantum key encapsulation mechanisms using Maude. PeerJ Comput. Sci. 9: e1547 (2023)

Formal Specification & Analysis of KEMs

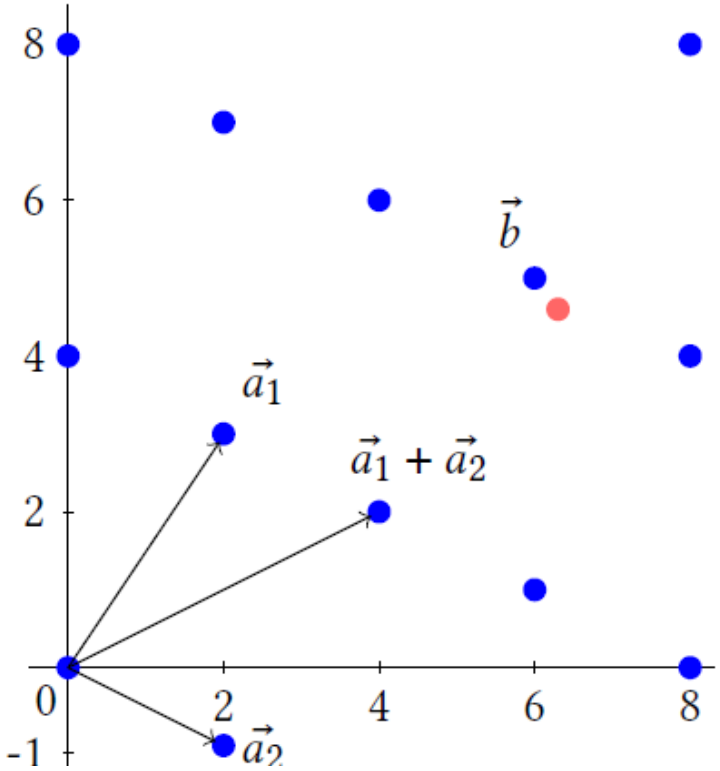
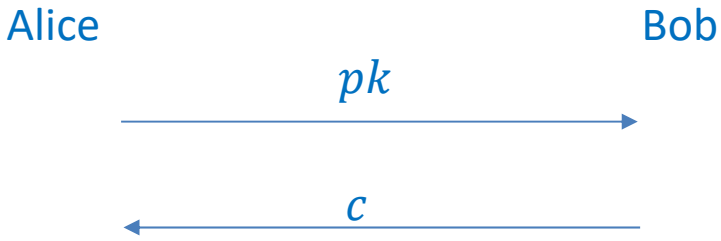


Fig. 2. An illustration of the closest vector problem in 2-dimensional lattice $\mathcal{L}\{\vec{a}_1, \vec{a}_2\}$, where $\vec{a}_1 = (2, 3)$ and $\vec{a}_2 = (2, -1)$



Definition 3.1. A key encapsulation mechanism (KEM) is a tuple of algorithms (`KeyGen`, `Encaps`, `Decaps`) along with a finite key space $\mathcal{K}$:

- `KeyGen`() $\rightarrow (pk, sk)$: A probabilistic *key generation* algorithm that outputs a public key pk and a secret key sk.
- `Encaps`(pk) $\rightarrow (c, k)$: A probabilistic *encapsulation* algorithm that takes as input a public key pk, and outputs an encapsulation (or ciphertext) c and a shared secret $k \in \mathcal{K}$.
- `Decaps`(c, sk) $\rightarrow k$: A (usually deterministic) *decapsulation* algorithm that takes as inputs a ciphertext c and a secret key sk, and outputs a shared secret $k \in \mathcal{K}$.

Formal Specification & Analysis of KEMs

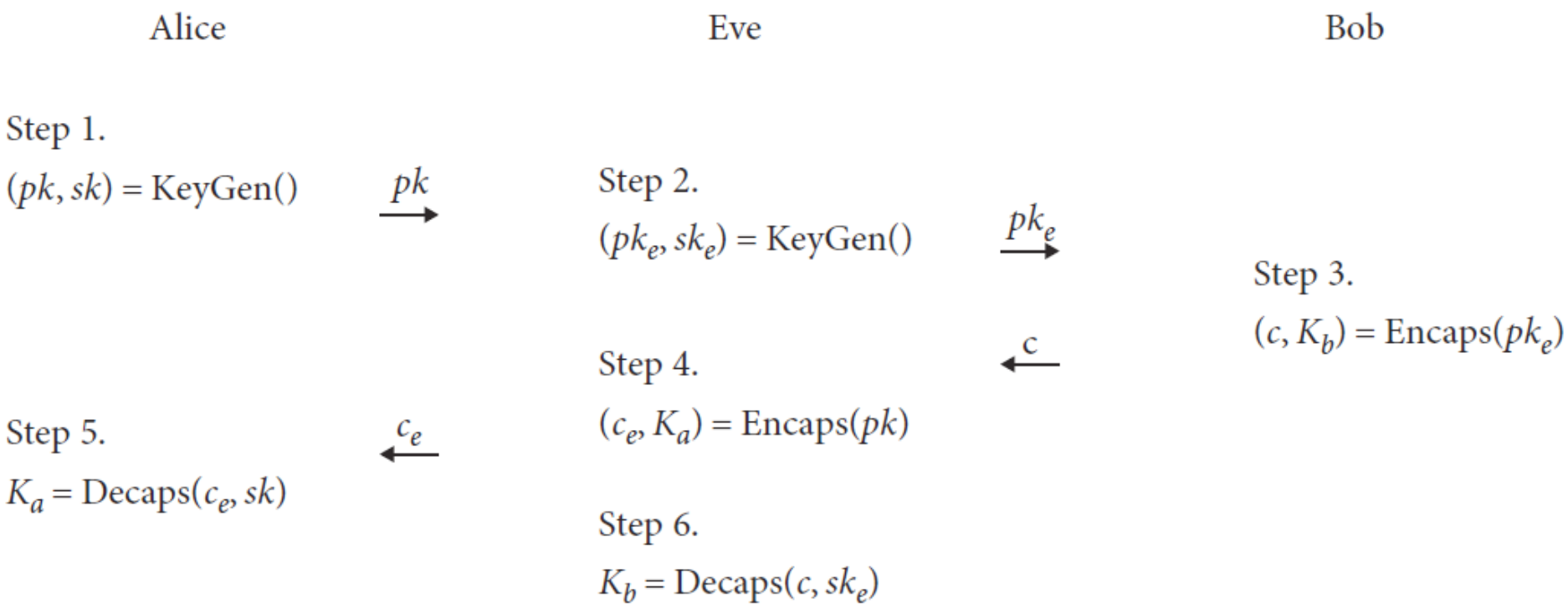


FIGURE 7: High-level representation of attacks.

Formal Specification & Analysis of KEMs

(i) a novel framework for the specification of post-quantum cryptographic protocols using Maude

(ii) an extended analysis of three post-quantum KEM protocols using model checking

(iii) verification of the presence of a man-in-the-middle attack in the three selected KEMs

(iv) discovery of a design flaw in BIKE (Bit Flipping Key Encapsulation), allowing a malicious participant to use a weak key to impersonate another participant

Formal Specification & Analysis of KEMs

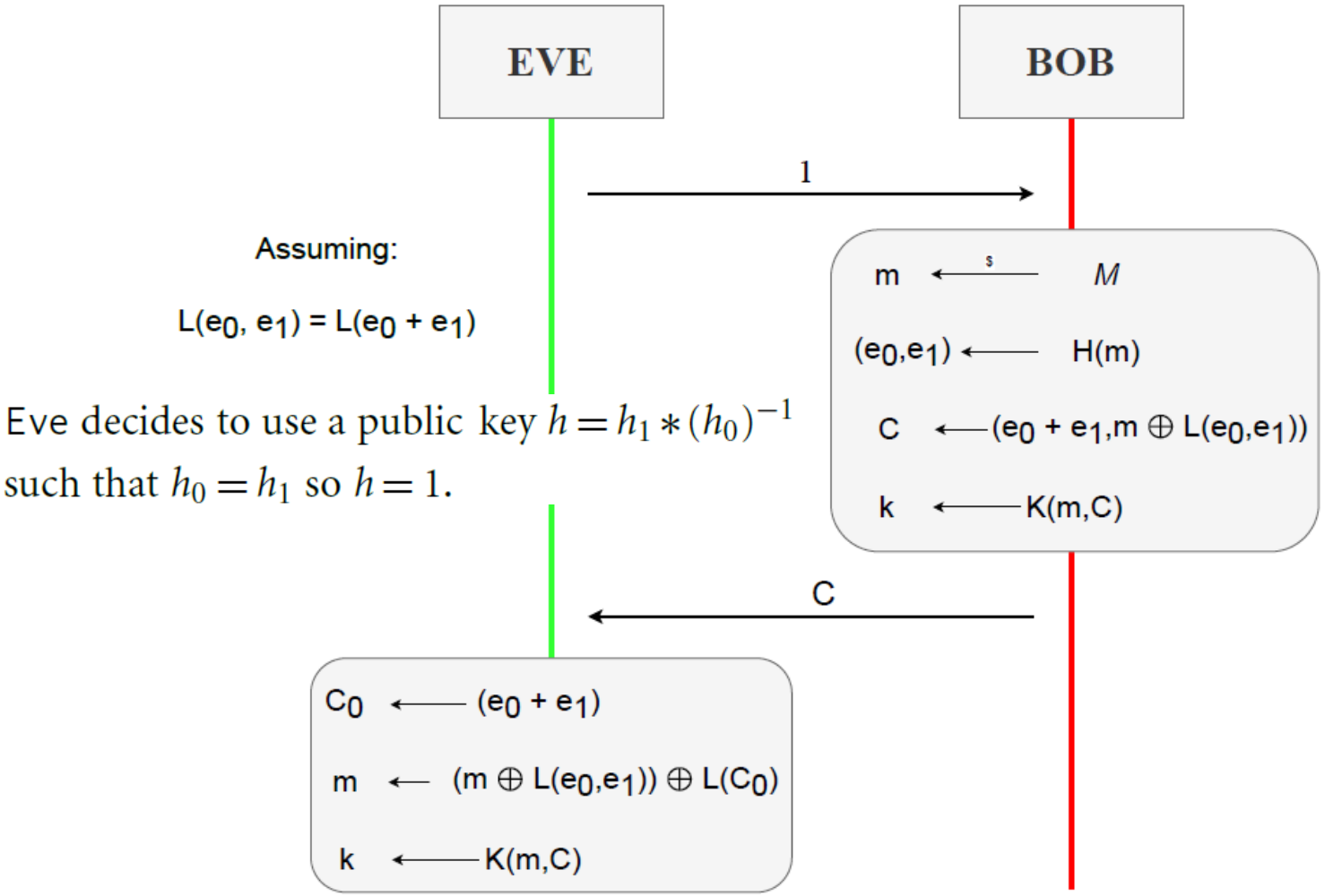
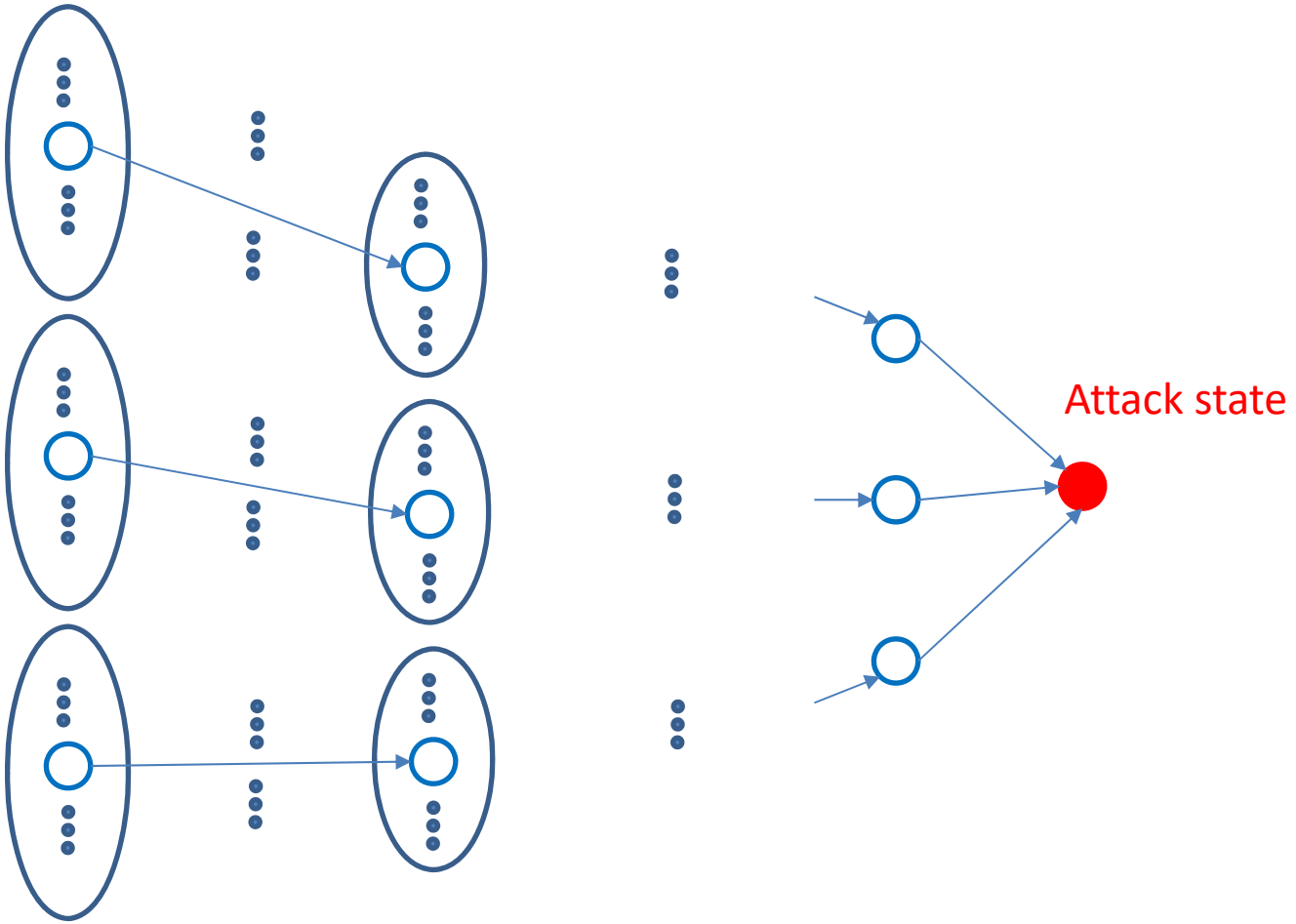


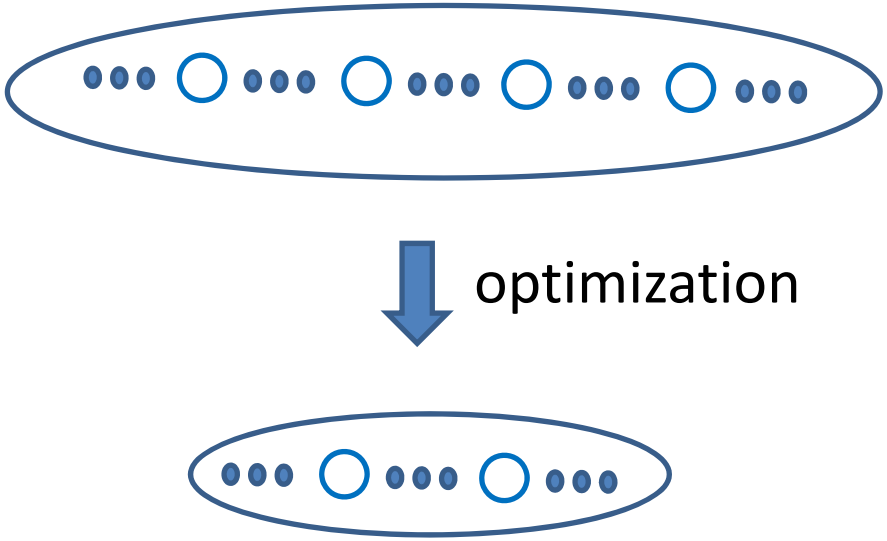
Figure 44 Diagram depicting a step trace in the BIKE symbolic model leading to the leakage of critical information.

Tools Developed

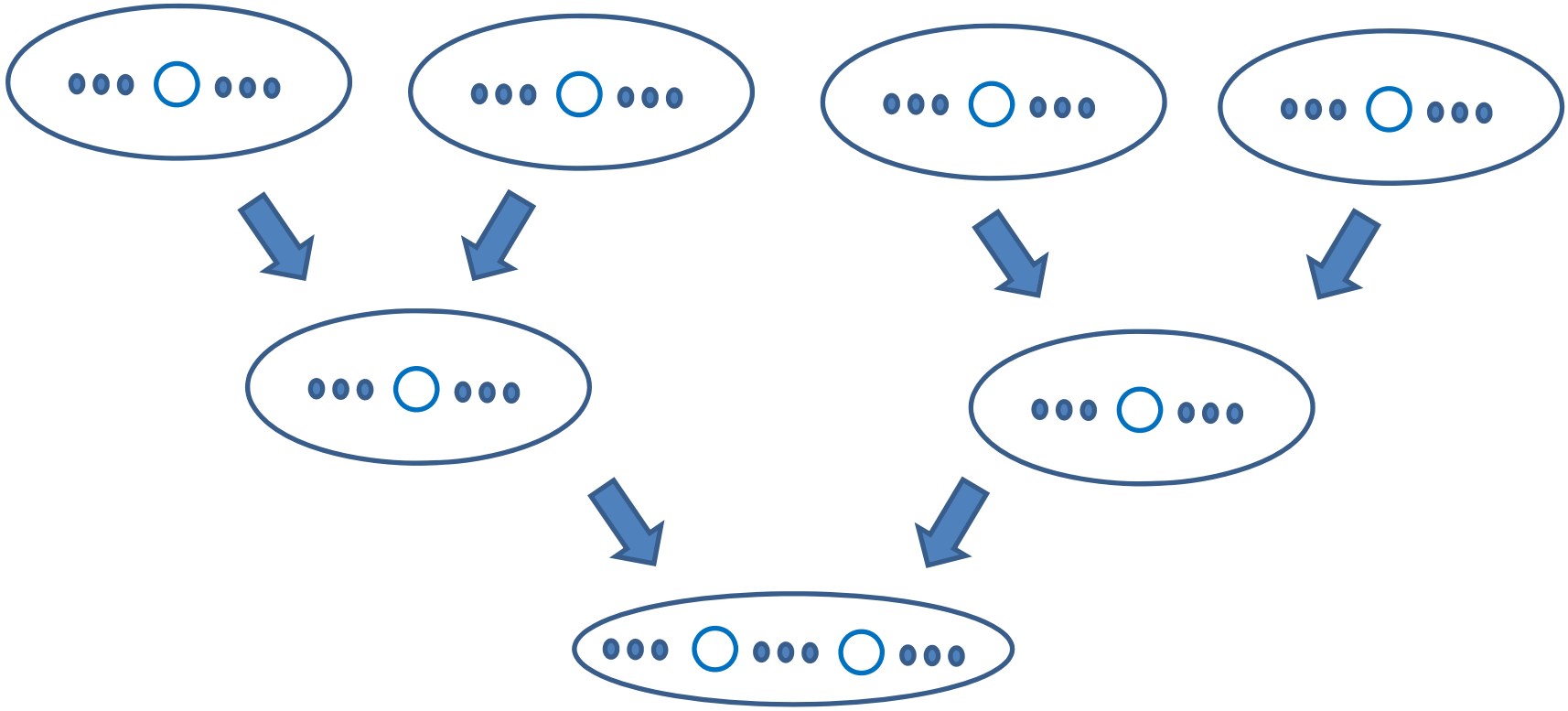
C.M. Do, A. Riesco, S. Escobar and K. Ogata: Parallel Maude-NPA for Cryptographic Protocol Analysis, 14th International Workshop on Rewriting Logic and its Applications (WRLA 2022), LNCS 13252, Springer, pp.253-273, (2022).



Tools Developed



Tools Developed



C.M. Do, A. Riesco, S. Escobar and K. Ogata: Parallel Maude-NPA for Cryptographic Protocol Analysis (an extended version of the WRLA 2022 paper), under review for journal publication

Tools Developed

D.D. Tran, K. Ogata: Formal verification of TLS 1.2 by automatically generating proof scores, Computers & Security 123: 102909 (1 - 15), Elsevier, (2022)

Invariant Proof Score Generator (IPSG)

Formal specification
An invariant property to prove
Lemmas

Proof scores of the invariant property & lemmas

Tools Developed

Proof is done by

(1) Structural induction of the reachable state space of a state machine formalizing a security protocol together with the intruder or attacker
(2) Case splitting
(3) Use of lemmas

Case splitting is conducted so that either true or false is returned for each sub-case

For each case such that false is returned, IPSG tries to use instances of some lemmas so that the sub-case is discharged

If IPSG cannot discharge such a sub-case, humans are supposed to take a close look at the assumptions (equations) used in the sub-case and conjecture lemmas

Formal Verification of PQ Protocols

D.D. Tran, C.M. Do, S. Escobar, K. Ogata: Hybrid post-quantum Transport Layer Security formal analysis in Maude-NPA and its parallel version. PeerJ Comput. Sci. 9: e1556 (2023)

Hybrid post-quantum Transport Layer Security (Hybrid PQ TLS) uses both the elliptic curve Diffie–Hellman key exchange and PQ KEM

It is supposed that the intruder can break the elliptic curve Diffie-Hellman key exchange, while she cannot break PQ KEM

Table 1 **Experimental results of the three attack patterns after 1,722h 20m 23s.**

Attack number	Maude-NPA			Par-Maude-NPA		
	Time (h:m:s)	Depth	Result	Time (h:m:s)	Depth	Result
0	1,722:20:23	H 11	∅	1,722:20:23	F 12	×
1	1,722:20:23	H 11	∅	1,722:20:23	H 13	∅
2	1,722:20:23	H 18	∅	1,722:20:23	H 19	∅

Formal Verification of PQ Protocols

Table 3 Comparison of Maude-NPA and Par-Maude-NPA in terms of running performance.

Attack number	Bounded depth	Maude-NPA Time (h:m:s)	Par-Maude-NPA #workers	Par-Maude-NPA Time (h:m:s)	Improvement (how faster)
0	8	70:39:03	8	18:46:37	3.8x
			12	16:54:15	4.2x
			16	15:26:02	4.6x
0	9	304:01:08	8	57:27:42	5.3x
			12	54:15:12	5.6x
			16	41:38:10	7.3x

Formal Verification of PQ Protocols

D.D. Tran, K. Ogata, S. Escobar, S. Akleylek, A. Otmani: Symbolic verification of Hybrid Post-Quantum TLS 1.2, under review for journal publication

D.D. Tran, K. Ogata, S. Escobar, S. Akleylek, A. Otmani: Formal analysis of Post-Quantum Hybrid Key Exchange SSH Transport Layer Protocol, under review for journal publication

Formal verification conducted is interactive theorem proving

The protocols formally specified in CafeOBJ

IPSG used to automatically generate proof scores

Lemmas conjectured by Duong by taking a close look at each case for which false is returned

Formal Verification of PQ Protocols

version exchange	VERSION_EX	$C \rightarrow S:$	Version_C
	VERSION_EX	$S \rightarrow C:$	Version_S
key exchange algorithms	KEX_ALGR	$C \rightarrow S:$	Suites_C
	KEX_ALGR	$S \rightarrow C:$	Suites_S
key exchange initiation	KEX_HBR_INIT	$C \rightarrow S:$	$\text{ECDH}_{\text{PK}_C}, \text{KEM}_{\text{PK}_C}$
key exchange reply	KEX_HBR_REPLY	$S \rightarrow C:$	$\text{LK}_S, \text{ECDH}_{\text{PK}_S}, \text{KEM}_{C_S}, \text{SIGN}$

Fig. 3. Messages exchanged in the PQ SSH protocol

Formal Verification of PQ Protocols

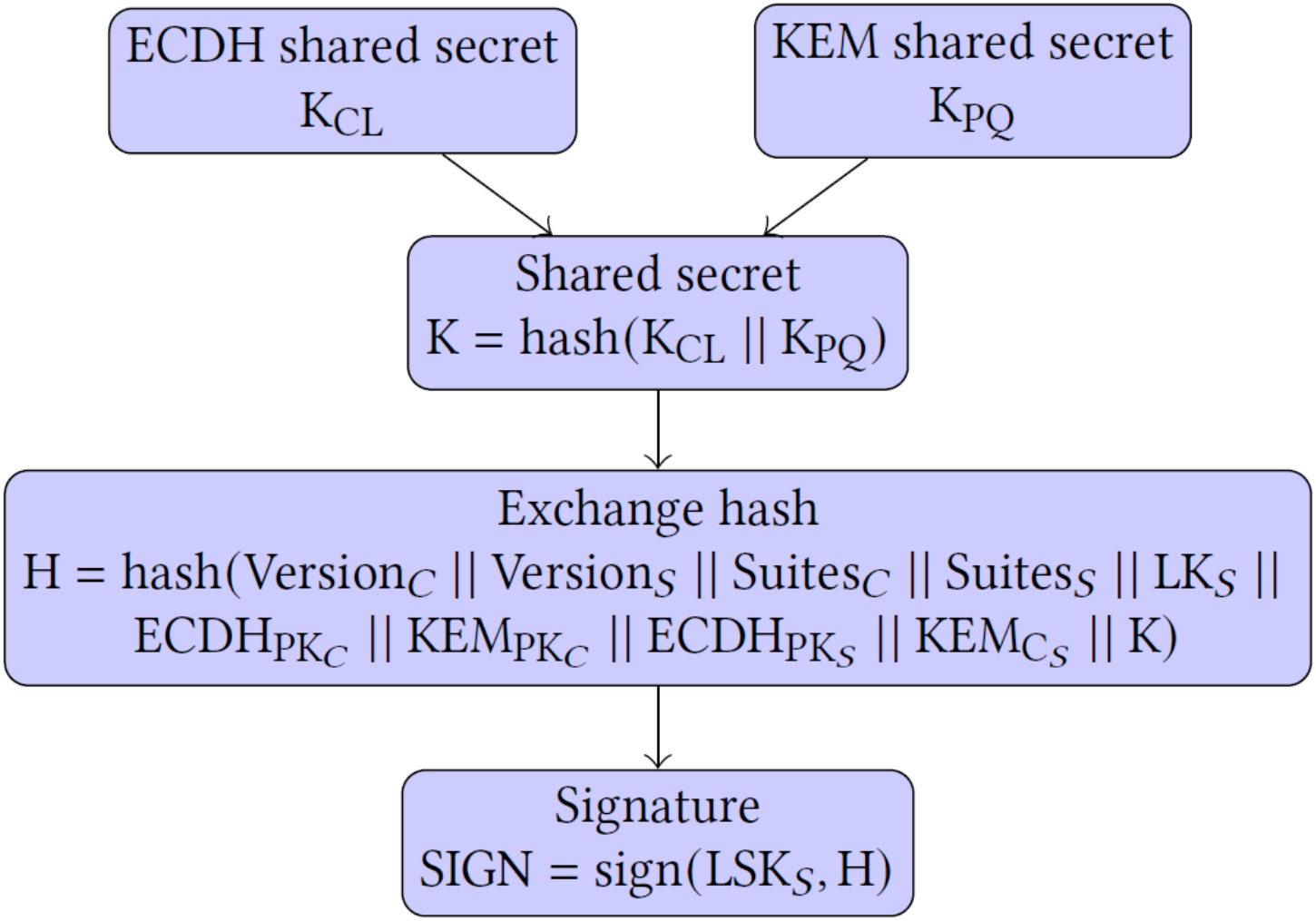


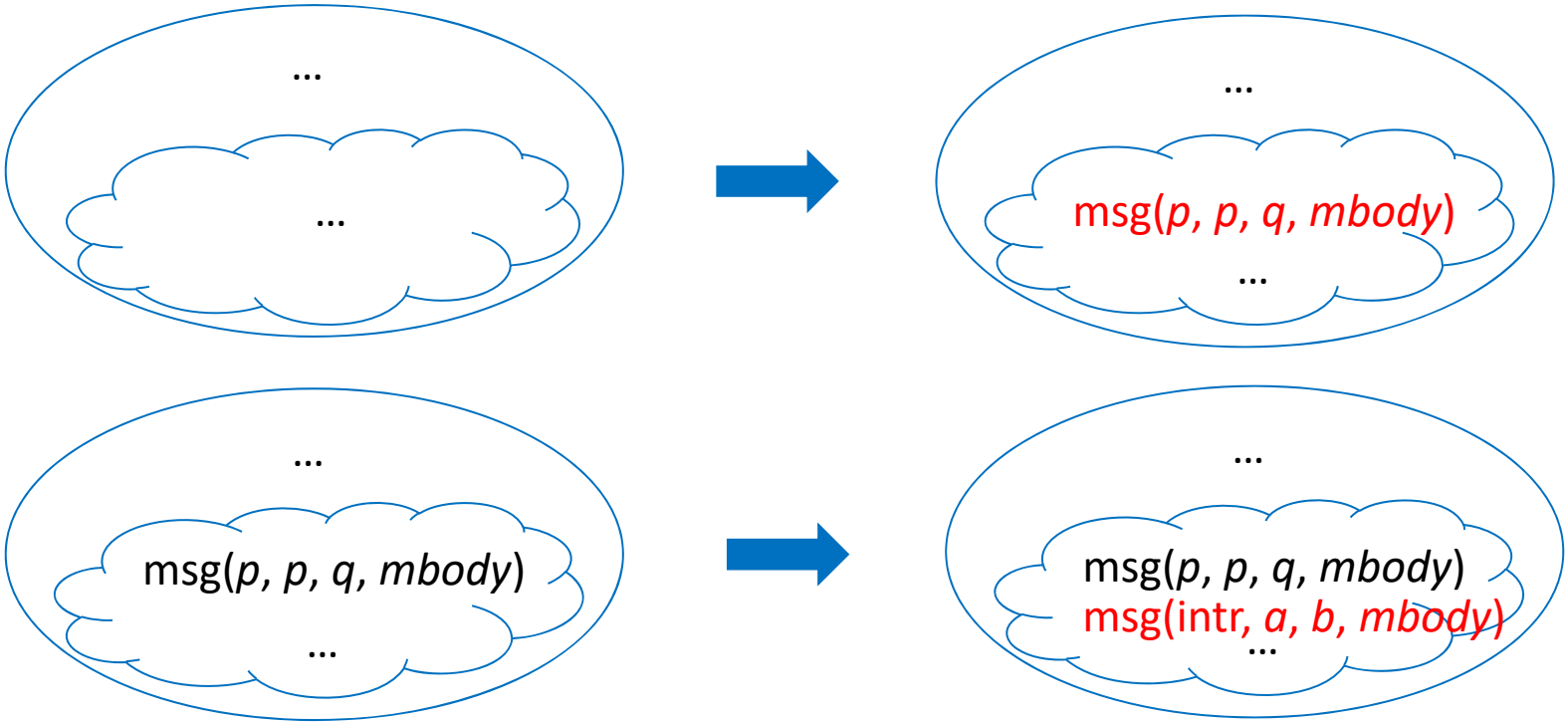
Fig. 4. Exchange hash and signature calculation

Formal Verification of PQ Protocols

- A state machine $M \triangleq \langle S, I, T \rangle$, where S is a set of states, $I \subseteq S$ is the set of initial states, and $T \subseteq S \times S$ is a set of state transitions
- Reachable states (R) : (1) $I \subseteq R$, (2) if $s \in R$ and $(s, s') \in T$, then $s' \in R$
- A state predicate p s.t. $(\forall s \in R) p(s)$, namely that it holds in all reachable states, is called an invariant property
- Many security properties, such as secrecy property and authentication property, can be expressed as invariant properties

Formal Verification of PQ Protocols

- Actions of ordinary participants and the intruder, such as sending messages, gathering information, faking messages, are formalized as state transitions.



Formal Verification of PQ Protocols

Step-1	A	$A \rightarrow B$:	$\mathrm{ECDH_{PK}} \,\|\|\, \mathrm{KEM_{PK}}$
Step-2	I	learns	$\mathrm{ECDH_{PK}} \,\|\|\, \mathrm{KEM_{PK}}$
Step-3	I	$A_2 \rightarrow B$:	$\mathrm{ECDH_{PK}} \,\|\|\, \mathrm{KEM_{PK}}$
Step-4	B	$B \rightarrow A_2$:	$\mathrm{LK}_B \,\|\|\, \mathrm{ECDH_{PK_2}} \,\|\|\, \mathrm{KEM_C} \,\|\|\, \mathrm{SIGN}$
Step-5	I	learns	$\mathrm{LK}_B \,\|\|\, \mathrm{ECDH_{PK_2}} \,\|\|\, \mathrm{KEM_C} \,\|\|\, \mathrm{SIGN}$
Step-6	I	$B \rightarrow A$:	$\mathrm{LK}_B \,\|\|\, \mathrm{ECDH_{PK_2}} \,\|\|\, \mathrm{KEM_C} \,\|\|\, \mathrm{SIGN}$

where I denotes the intruder

Fig. 5. Counterexample of auth

Formal Verification of PQ Protocols

$$H = \text{hash}(\text{Version}_C \,||\, \text{Version}_S \,||\, \text{Suites}_C \,||\, \text{Suites}_S \,||\, \text{LK}_S$$
$$||\, \text{ECDH}_{\text{PK}_C} \,||\, \text{KEM}_{\text{PK}_C} \,||\, \text{ECDH}_{\text{PK}_S} \,||\, \text{KEM}_{C_S} \,||\, \text{K} \,||\, \text{A} \,||\, \text{B})$$

Client and server identifications added

Events

- The 1st International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols
  - Held in Madrid, Spain on Oct 24th, 2022 as a satellite event of ICFEM 2022
- A special issue of FAVPQC 2022 at PeerJ Computer Science (Q2 for 2021 – 2022, Q1 for 2017 – 2020)
- The 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols
  - Held in Brisbane, Australia on Nov 21st, 2023 as a satellite event of ICFEM 2023

Some future directions

- A more generic intruder model that can be used for formal verification of other PQ security protocols
- More case studies of PQ protocol formal verification
- Automatic/systematic lemma conjecture
- Making IPSG more scalable

Some future directions

- Formal verification of quantum security protocols in which quantum cryptographic primitives, such as BB84, are used, including an intruder model for it
- To this end, we need to comprehend quantum circuits/protocols/programs better, for which we have been working on formal verification of quantum circuits/protocols/programs
- …

Acknowledgement

The staff members of the four funding agencies (JST, CNRS, AEI and TUBITAK) and the four universities (JASIT, Polytechnic University of Valencia, University of Rouen Normandie and Ondokuz Mayis University) have always supported FAVPQC.

We appreciate their efforts and time.

Dr. Yuzuru Tanaka has always encouraged us to conduct good research.

We are grateful to him for his endless encouragement.

Thank you for listening!