G5448 – Secure Communication in the Quantum Era

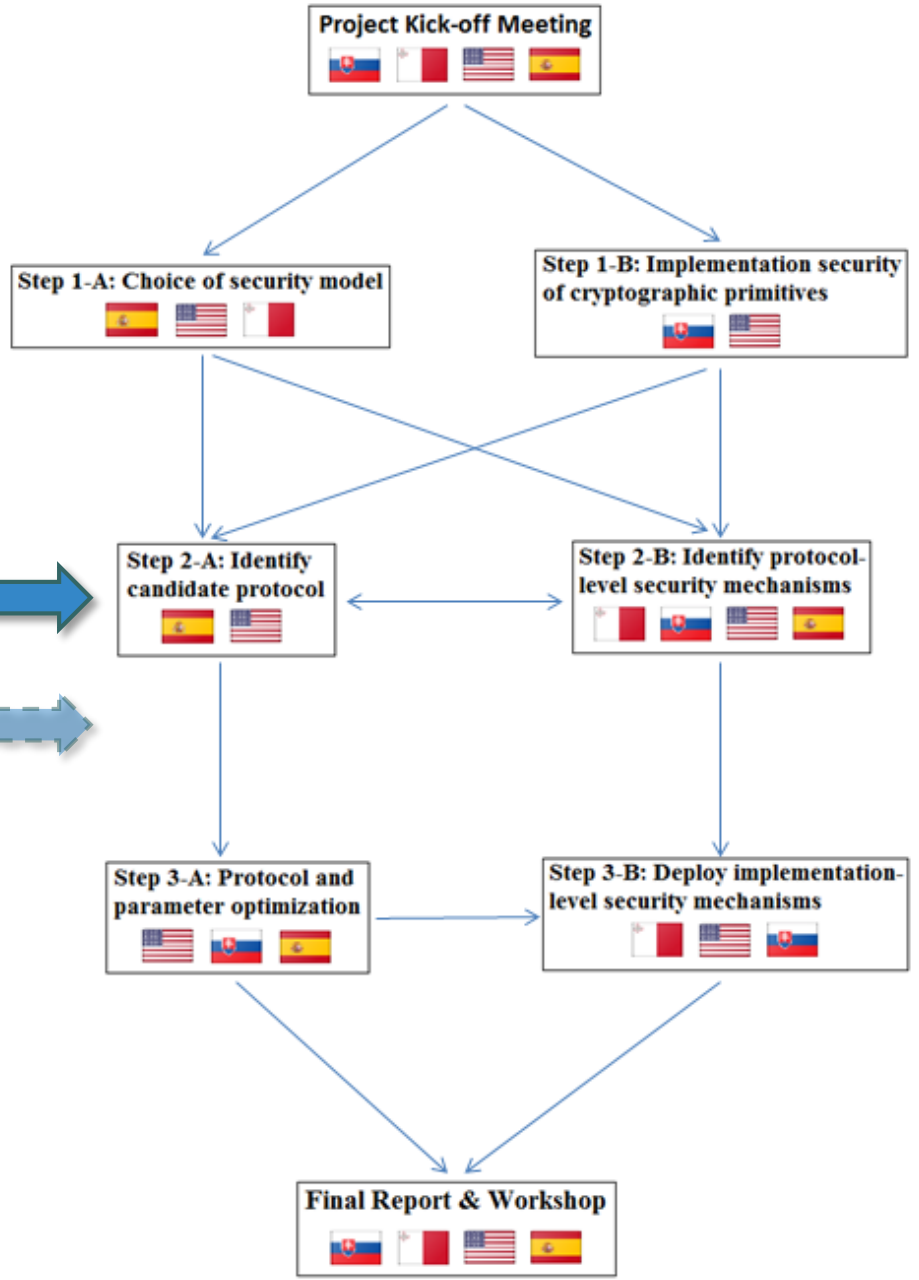
Florida Atlantic University – CAE-R


Rainer Steinwandt

Building blocks for secure post-quantum communication

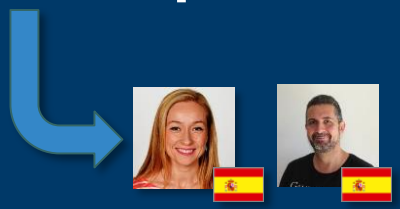
Research thrusts

- Protocol designs for post- & future quantum group key establishment
- Quantifying post-quantum security margins



Post-quantum group key establishment

- Generic design (“compiler”) requiring
  - post-quantum signature
  - post-quantum key encapsulation
- Design minimizes number of signatures
- **Option for eventual transition from future quantum to post-quantum**



entropy

MDPI

Article

From Key Encapsulation to Authenticated Group Key Establishment—A Compiler for Post-Quantum Primitives †

Edoardo Persichetti [1,‡], Rainer Steinwandt [1,‡] and Adriana Suárez Corona [2,*,‡]

1 Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL 33431, USA; epersichetti@fau.edu (E.P.); rsteinwa@fau.edu (R.S.)
2 Department of Mathematical Sciences, Universidad de León, 24071 León, Spain
* Correspondence: asuac@unileon.es
† This paper is an extended version of our paper published in JNIC 2019 (as 2-page extended abstract and as poster) held at the San Francisco de Cáceres Complex between June 5 and 7, 2019.
‡ These authors contributed equally to this work.

Received: 30 September 2019; Accepted: 27 November 2019; Published: 30 November 2019

check for updates

Abstract: Assuming the availability of an existentially unforgeable signature scheme and an (IND- CCA secure) key encapsulation mechanism, we present a generic construction for group key establishment. The construction is designed with existing proposals for post-quantum cryptography in mind. Applied with such existing proposals and assuming their security, we obtain a quantum-safe three-round protocol for authenticated group key establishment that requires only one signature per protocol participant.

Keywords: authenticated group key establishment; post-quantum cryptography; key encapsulation mechanism

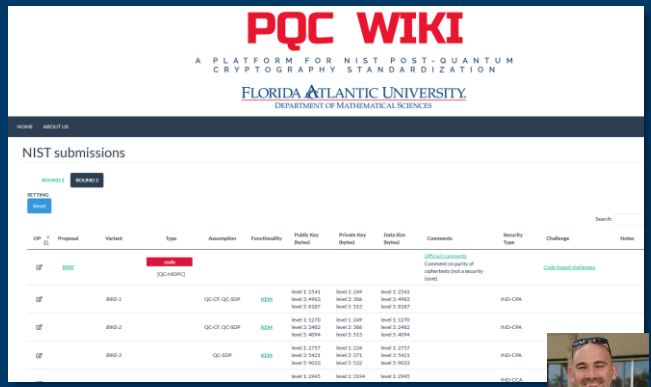
1. Introduction

To enable confidential communication among a group of two or more users over an insecure network, cryptography provides group key establishment procotols. Dealing with a non-trusted communication infrastructure, the question of authenticating protocol participants naturally arises in this context as well. The resulting cryptographic protocols are commonly application-agnostic and focus only on the task of establishing a shared high-entropy secret among the legitimate users, not mandating any particular usage of that secret key in subsequent applications. The resulting task, authenticated group key establishment (AGKE), is fairly well-understood, even though there is a remarkable diversity in the details of security models in use. A standard technique to derive an AGKE solution is to apply some form of protocol compiler or generic framework to a passively secure solution. If a public-key infrastructure is available, signatures provide an adequate mechanism. This results commonly in protocols with a substantial number of signatures being computed, transmitted, and verified:

- In the Katz-Yung compiler [1], for each message sent in the original protocol, a signature has to be computed and transmitted (and verified). For instance, Apon et al. [2] propose the application of this compiler for their unauthenticated group key establishment solution.
- The compiler made by Bresson et al., C-AMA [3] requires a signature for each message in the original protocol, plus one more for each protocol participant (and according signature verifications).
- Bohli’s framework for robust group key agreement [4] targets two-round protocols, and in each round each participant sends a signed message (and verifies signatures by all other participants).

Building blocks & parameter suggestions

- Candidate selection informed through NIST's ongoing standardization effort



pqc-wiki.fau.edu

- Research on:
  - Public-key encryption with LWE-type assumption
    → ASIACRYPT 2019

  - Reliably estimating cost to solve LWE problem
    → AFRICACRYPT 2019

Resource estimates for quantum attacks

- Future quantum (Diffie-Hellman) parameters informed by quantum computing report for Federal Office for Information Security

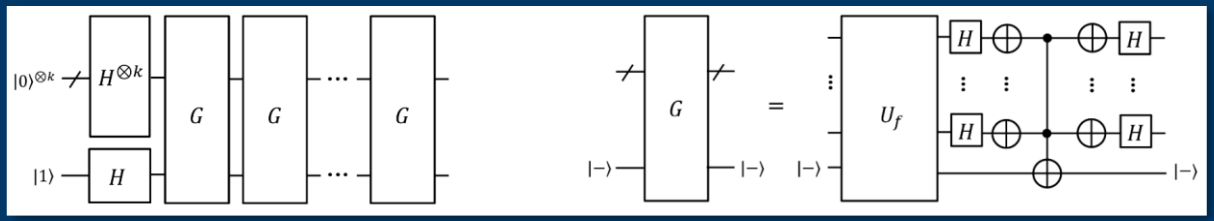
- Post-quantum parameter choices?

> Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a k-bit key (e.g. AESk)

Submission Requirements and Evaluation Criteria for NIST's ongoing Post-Quantum Cryptography Standardization Process

Quantum resources for a key search*

- **Key parameters:**
  - #qubits
  - circuit depth
  - #gates, especially T-gates



- **Essential cost determined by Grover's algorithm:**
  - number of steps exponential in key length
  - cost of each step depends on resources for implementing the target cipher as quantum circuit

* attacks in stronger attack models can be considered, e.g., Bonnetain et al. 2019, but for our purposes, key search is of specific interest

S-box implementation determines cost

`SubByte` is only source of T-gates in AES

- **Prior work:** directly translate algebraic description of S-box into quantum circuit
- **Here:** reduce #T-gates by exploiting classical circuit optimization by Boyar-Peralta


IEEE Transactions on Quantum Engineering

Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit

BRANDON LANGENBERG[1,2], HAI PHAM[1,3], AND RAINER STEINWANDT[4]

ABSTRACT To quantify security levels in a postquantum scenario, it is common to use the quantum resources needed to attack the Advanced Encryption Standard (AES) as a reference value. Specifically, in the National Institute of Standards and Technology's ongoing postquantum standardization effort, different security categories are defined that reflect the quantum resources needed to attack AES-128, AES-192, and AES-256. This article presents a quantum circuit to implement the S-box of AES. Also, leveraging an improved implementation of the key expansion, we identify new quantum circuits for all three AES key lengths. For AES-128, the number of Toffoli gates can be reduced by more than 88% compared to Almazrooie et al.'s and Grassl et al.'s estimates while simultaneously reducing the number of qubits. Our circuits can be used to simplify a Grover-based key search for AES.

INDEX TERMS Advanced Encryption Standard (AES), Grover's algorithm, quantum circuit, quantum cryptanalysis, quantum engineering.

I. INTRODUCTION

Reacting to progress in the development of quantum computers, the National Institute of Standards and Technology (NIST) has initiated a process to standardize cryptographic primitives that are designed to remain secure in the presence of large-scale quantum computers [15]. To fix security categories, NIST's call for proposals offers the quantum resources for an exhaustive key search in the case of AES-128, AES-192, and AES-256 as a reference point. Relevant cost measures include the number of qubits, the number of T- and Clifford gates, and the T-depth. It is not hard to see that with exception of the highly structured S-box—the `SubBytes` transform—all of the Advanced Encryption Standards (AES) can be implemented by means of NOT and CNOT gates.

A. CONTRIBUTIONS

In the following, we present a new quantum circuit to implement `SubBytes`, which builds on a result by Boyar and Peralta [7]. This approach allows a substantial reduction in the number of T-gates compared to the quantum circuits proposed by Grassl et al. [9] and, more recently, by Almazrooie et al. [1]. Our circuit requires 32 qubits, 55 Toffoli gates, 314 CNOT gates, 4 NOT gates, Toffoli depth 40, and a total [neutral current transformer (NCT)] depth of 298, including "cleaning up" ancillas—a reduction of the Toffoli count by more than 88%. There are different options to compile Toffoli gates into Clifford and T gates, and the common quantum cryptanalytic approach is to first express AES as an NCT circuit, i.e., with NOT, CNOT, and Toffoli gates. Consequently, in this article, we stay at the NCT level, leaving the choice of a particular decomposition of Toffoli gates into more elementary building blocks to a subsequent synthesis step.

Moreover, building on [1] and [9], we present new quantum circuits for all three standardized key lengths of AES, which simultaneously offer savings in the number of qubits, the number of Toffoli gates, and the number of Clifford gates.

B. ORGANIZATION

First, we briefly recall the structure of the S-box of AES and survey prior work to express this functionality as a quantum circuit. Thereafter, we present our design for implementing `SubBytes` in the NCT gate set and integrate it into quantum circuits for AES-128, AES-192, and AES-256. We conclude

VOLUME 1, 2020 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/ 2500112

Improved quantum key search for AES
$\rightarrow$ IEEE Trans. on Quantum Engineering vol. 1, 2020

- Jaques et al.: use AND gates to reduce #T-gates, reduce depth and T-depth (at the cost of more qubits)

Moving forward

- Focus student involvement on
  - Protocol level: Floyd Johnson
    ($\rightarrow$ to attend PQCrypto 2020)

  - Parameter analysis: Shaun Miller
    ($\rightarrow$ lattice reduction)

- Focus analysis and optimization on identified target protocol (informed by implementation needs)