AFRL-RI-RS-TR-2018-184

QUANTUM TECHNOLOGY, HIGH SPEED ENCRYPTION AND GLOBAL ANALYSIS OF NETWORKS

FLORIDA ATLANTIC UNIVERSITY

AUGUST 2018

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2018-184 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
PAUL M. ALSING
Work Unit Manager

/ S /
JOSEPH A. CAROLI
Acting Technical Advisor
Computing & Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
AUGUST 2018	FINAL TECHNICAL REPORT	FEB 2015 – FEB 2018

4. TITLE AND SUBTITLE

QUANTUM TECHNOLOGY, HIGH SPEED ENCRYPTION AND GLOBAL ANALYSIS OF NETWORKS

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
FA8750-15-2-0047

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)

Warner A. Miller, Rainer Steinwandt

5d. PROJECT NUMBER
T2QL

5e. TASK NUMBER
FL

5f. WORK UNIT NUMBER
AT

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Florida Atlantic University
777 Glades Road
Boca Raton FL 33431

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RITA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2018-184

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The objectives of this research to address three aspects of complex communication networks. First, for point-to-point connections we will assess the resources for attacking state-of-the art block ciphers, specifically the Advanced Encryption Standard (AES) with standardized key lengths and other AES finalists with a quantum computer. Second, we explore the integration of classical cryptographic techniques into the $\alpha\eta$ scheme, and the potential of ``all-or-nothing transforms'' to obtain a hybrid (classical-quantum) scheme with higher throughput than αη. Finally, we will apply curvature flow to complex communication networks in 3D in order to characterize their global topological and geometric properties. We will evolve networks under curvature flow with surgery to characterize its structure. We will examine curvature heat-maps to give new insight on the realization that positive curvature regions in networks signal load balance, while negative curvature regions identify congestion in the network.

15. SUBJECT TERMS

Ricci Flow, Discrete Ricci Flow, Graph Curvature, Graph Ricci Flow

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			PAUL M. ALSING
U	U	U	UU	33	19b. TELEPHONE NUMBER (*Include area code*)

Contents

1 SUMMARY **1**

2 INTRODUCTION **1**
2.1 Introduction to quantum-safe encryption of point-to-point connections 1
2.2 Introduction to Global analysis of Networks 3

3 METHODS, ASSUMPTIONS AND PROCEDURES **4**
3.1 Five Metrics and Milestones and Accomplishments. 4
3.2 Publications Under this Effort 5

4 RESULTS AND DISCUSSION **6**
4.1 Security of Point-to-Point Connections 6
4.1.1 Resource Estimates for Quantum Attacks 7
4.1.2 Enhancing $\alpha\eta$ through the Integration of Classical Cryptographic Techniques 10
4.2 Global Analysis of Complex Networks 12
4.2.1 The 3-Dimensional Neck Pinch Model 14
4.2.2 DRF with Surgery: A Numerical Realization of Thurston's Geometrization for a Neck Pinch Geometry. 17
4.2.3 From Piecewise Linear Curvature to Graph Curvature 18
4.2.4 An Example Application to a Real World Network: Curvature Heat Maps . 19
4.2.5 Wang and Yau's Quasi Local Mass 20

5 CONCLUSIONS **22**

6 LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS **24**

7 REFERENCES **25**

List of Figures

1 The parallel Grover oracle computes the encryption for all plaintexts in parallel. . . 7
2 The sequential Grover oracle trades qubits for circuit depth. 8
3 Structure of a quantum circuit for AES. 9
4 Quantum circuits for SERPENT's S-boxes: even permutations. 9
5 Quantum circuits for SERPENT's S-boxes: odd permutatons 10
6 Schematic overview of the hybrid protocol. 12
7 The data structure of an edge ($e = \overline{v_1 v_2}$) used in our definition of the Forman-Ricci tensor. 14
8 A two dimensional representation of the 3D neck pinch geometry of Angenent and Knopf (continuum on top, and discrete on bottom). 15
9 An illustration of the icosahedron neck pinch geometry for nine cross-sectional icosahedra (top), and its dual dodecahedral lattice (bottom). 16
10 The RF of a lopsided neck pinch geometry through the Type-1 singularity using surgery and yielding the geometry as a direct product of two 3-spheres. 16
11 A 2-dimensional cross section of a lopsided neck pinch geometry evolving under RF through the Type-1 singularity. 17
12 After the manifold surgery the lobe was closed using a spherical cap with proper matching conditions as illustrated in this figure. 18
13 *Seven-node e-mail sub-network based on seven e-mail exchangers collected over several years.* 20
14 *Modified Forman Ricci curvature map (Eq. 14) for the graph illustrated in Fig. 13.* 21
15 *Isometric embedding of the spherical Boyer-Lindquist surface for $R = 3/2M$ into Minkowski spacetime.* 21
16 *Landscape of the Wang-Yau quasi-local energy for a sphere around a Kerr black hole in the space of the first two Fourier coefficients a_1 and a_3.* 22

1 SUMMARY

The objectives of this research were to address three aspects of complex communication networks. The first area was point-to-point connections while the second dealt with global analysis of the network geometry and topology.

- *Point-to-point connections.* In this area of research we assessed the resources for attacking state-of-the art block ciphers with a quantum computer. Specifically, Grover-based attacks against the Advanced Encryption Standard (AES), the AES finalists MARS and Serpent, and the NSA-designed lightweight block cipher families SIMON and SPECK were considered. Based on our resource analyses, we are in a position to recommend a block cipher that can be expected to remain secure with scalable quantum computers being available to attackers. In addition, we explored the integration of classical cryptographic techniques into the $\alpha\eta$ scheme. We showed how to integrate a"restricted" all-or-nothing transform to obtain an efficient hybrid (classical-quantum) scheme with (provable) information-theoretic security guarantees. Combining our design with a classical high-performance solution for authenticated encryption with associated data (AEAD)—we considered the ChaCha20 stream cipher and Poly1305 authenticator—results in a highly performant encryption solution with security guarantees that go beyond established classical security models.

- *Network Geometry and Topology.* We applied our discrete Ricci flow (DRF) approach to embedded communication networks in 3D in order to characterize and analyze its global topological and geometric properties, and to identify this structure with the function of the communication network. In particular, we simulated the evolution of embedded networks under DRF, provided surgery and characterized its topological structure. We are in a position to use this discrete curvature analysis to construct a quasi local measure of congestion (QLC) that will be based on our discrete quasi-local mass (QLM) results in this effort. We examined curvature heat-maps using Foreman curvature, and our results give new insight on the realization that positive curvature regions in networks signal load balance, while negative curvature regions identify congestion in the network. We diagonalized the discrete Ricci flow equations so that they have favorable linear scaling.

2 INTRODUCTION

In this section we introduce both the point-to-point connection analysis followed by an introduction to global analysis of networks and discrete Ricci flow.

2.1 Introduction to quantum-safe encryption of point-to-point connections

Once large-scale quantum computing becomes available, the security margins of a number of established cryptographic solutions are reduced. Shor's seminal work [1] showed that for many deployed asymmetric solutions quantum algorithms invalidate the underlying hardness assumption. This led to ongoing efforts to transition to a national *post-quantum* standard for digital signatures and other asymmetric primitives [3]. For symmetric encryption, the situation appears less dramatic, as the most relevant quantum cryptanalytic improvement is based on a result by Grover [2], which offers asymptotically only a quadratic speed-up over a classical attack. In essence, Grover's algorithm enables an asymptotically faster exhaustive key search based on known plaintext-ciphertext pairs, but quantifying the exact cost of such a quantum attack is non-obvious, as a quantum circuit

needs to be implemented that depends on the target cipher. This results in a situation where the cost for attacking ciphers with the same secret key length can differ substantially, i.e., block ciphers with comparable classical characteristics may offer different resistance to quantum attacks. To quantify the resources of quantum attacks, this project considered the number of qubits, number of Clifford+T gates, circuit depth, and T-depth. The choice of these metrics with this particular set of quantum gates is motivated by the suitability for interfacing with state-of-the art techniques for quantum error correction (specifically, surface codes). We report here on the quantum resource analysis of several block ciphers:

- AES, arguably the most prominent block cipher in use today. The recognition of our quantum cryptanalytic results on this cipher [4] is evidenced by the National Institute of Standards and Technology (NIST)'s decision to use our results in the *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process* to characterize security strength categories [5].

- Two AES finalists, MARS and Serpent, which follow different design principles – one building on a large "random" S(ubstitution)-box, the other on small S-boxes. It turned out that MARS is substantially more demanding in being mapped to an efficient quantum circuit, and when adding NSA's lightweight designs SIMONand SPECK to the comparison, substantial cost differences became apparent [6].

Complementing its cryptanalytic role, quantum technology offers an attractive option for *designing and implementing* cryptographic solutions. We built on an existing protocol [7], commonly referred to as $\alpha\eta$, which seeks to leverage physical (channel) characteristics to establish security guarantees. Namely, $\alpha\eta$ aims at exploiting properties of coherent states of light to obtain secure data encryption over an optic channel. Its security is based on the uncertainty of any measurement of the transmitted coherent states due to the intrinsic quantum noise. This setting is not directly amenable to popular cryptographic models and techniques, where ciphertexts are modeled as (readily available) bitstrings. On the other hand, from an implementation cost perspective, use of the optic channel appears more elaborate than a standard communication channel.

In the project we showed how a particular type of bijection — an all-or-nothing-transform (AONT) — can be used to enhance $\alpha\eta$. Such maps are designed to hide partial information on their input as long as the output is not completely known. For our purposes, introducing a notion of *restricted* AONT turned out to be helpful. We used a restricted AONT for a pre- (and corresponding post-)processing step in $\alpha\eta$ to harness security guarantees of the latter without having to transmit the complete payload through the optic channel. Parts—in fact most—of the payload can be transmitted classically, maintaining security without introducing computational assumptions. For practical purposes, error correction needs to be considered in our design as well, and we will report on this aspect below. To have a provable argument conveniently available, in our work we restricted to a conceptually simple form of error correction. Finally, for actual deployment, our design would naturally be combined with a computationally secure AEAD primitive. This results in an encryption solution where already moderate bandwidth on the optic channel prevents an attacker from reliable *ciphertext* access, extending the security of an AEAD solution beyond what is captured by common classical security models. We also established a form of forward secrecy in our system design — even after compromise of the secret key, *past* transmissions still afford

secrecy guarantees. Again, we do not require the introduction of computational assumptions for this; our analysis is again based on an information-theoretic argument.

2.2 Introduction to Global analysis of Networks

Hamilton's Ricci flow (RF) yields new insights into a broad range of problems from Perelman's proof of the Poincaré conjecture to greedy-routing problems in cell phone networks [12, 13, 14, 15, 16]. Here the time evolution of the metric $\dot{\boldsymbol{g}}$ is proportional to the Ricci tensor $\boldsymbol{R}c$,

$$\dot{\boldsymbol{g}} = -2\, Rc\,(\boldsymbol{g})\,. \tag{1}$$

The RF equation yields a forced diffusion equation for the curvature; i.e., the scalar curvature (R) evolves as

$$\dot{R} = \triangle R + 2R^2, \tag{2}$$

here $\triangle$ is the Laplacian with respect to the metric $\boldsymbol{g}$.

The majority of the engineering applications of RF have been limited to the numerical evolution of piecewise linear surfaces [17]. This is not surprising since a geometry with complex topology is most naturally represented in a coordinate-free way by unstructured meshes, e.g. finite volume [18], finite element [19]. The applicability of discrete RF in two dimensions arises from its diffusive curvature properties and from the uniformization theorem for surfaces: every simply connected Riemann surface evolves under RF to one of three constant curvature surfaces — a sphere, a Euclidean plane or a hyperbolic plane. RF on surfaces is an accepted method for engineering a metric for a surface given only its curvature [17]. However, in three dimensions, it is significantly more complicated. In particular, singularities can form during evolution under RF. In three dimensions, the uniformization theorem yields the geometrization theorem of Thurston, that shows that each closed 3-manifold has a decomposition into a connected sum of one or more of eight prime 3-manifolds [20, 21]. The diffusive curvature flow in three and higher dimensions together with this classification provides a richer taxonomy than its 2-dimensional counterpart. Perhaps this more refined taxonomy may prove useful in network classification. Diffusive curvature flow may provide noise reduction in higher dimensional manifolds, and in this direction we are currently exploring a coupling of RF with persistent homology [22, 23]. Finally, the soliton solutions of RF are Ricci flat and are therefore vacuum solutions of Einstein's equations for gravitation. This feature and its connection to the renormalization group make RF with boundary an exciting topic for current research into AdS/CFT models of quantum gravity [24, 25].

In this area research we report on four major advances, extending our work on SRF to what we refer to as discrete Ricci flow (DRF):

- We diagonalized the SRF equations so that they are scalable to large data sets [47].
- We preformed the first DRF evolution through a curvature singularity in 3-dimensions using manifold surgery [48].
- We developed the first application to Wang and Yau's quasi-local energy using our techniques, and this has allowed us extend our research to defining a quasi-local congestion energy-functional for networks [49].
- We unified our curvature expressions with those of Forman, thus allowing us to extend our curvature flow analysis from discrete manifolds to complex networks [48].

One of our graduate students (S. Ray) was the first to apply the Wang and Yau formulation of quasi-local mass for an extreme rotating black hole [49]. He has been recruited as a National Research Corporation (NRC) postdoctoral fellow at AFRL/RIT. In Ray's work he showed the need to extend their definition to handle definitions below a critical radius above the horizon. This development was important in order for us to extend this novel mathematical framework to more general structures, in particular, to the measure of quasi-local congestion to complex networks. We are now in a position to move this forward. Our results are now being used by numerous groups to develop a discrete quasi-local measure of congestion in networks [49, 51, 52]. This quasi local congestion (QLC) measure could be an ideal filtration parameter to guide network reconfiguration and ensure load balance.

3 METHODS, ASSUMPTIONS AND PROCEDURES

3.1 Five Metrics and Milestones and Accomplishments.

We addressed each of the five primary tasks and technical requirements throughout this research effort as follows:

- *(Metric 4.1.1–4.1.3)* We derived quantum circuits and resource counts for quantum attacks against AES-128, AES-192, AES-256, MARS, and Serpent as planned. Based on these analyses, we can identify cipher characteristics that support "quantum resistance." Thus, instead of detailing RC6 and Twofish circuits, we collaborated with Y-K Liu and E Schoute, adding the lightweight designs SIMON and SPECK to the resource comparison. We identified a cipher-agnostic resource saving/trade-off for handling plaintext-ciphertext pairs in Grover's algorithm.

- *(Metric 4.2.1–4.2.3)* Leveraging an AONT, we reduced $\alpha\eta$'s implementation complexity. Only a part of the preprocessed payload needs to be sent via the optic channel to ensure information-theoretic guarantees, including a provable forward secrecy guarantee. For self-synchronization of the classical transmission, existing techniques suffice. For the optic channel, a simple preprocessing is incompatible with the benefits from the AONT, but with the reduced bandwidth need, our error correction on the optic channel appears adequate.

- *(Metric 4.3.1–4.3.3)* We successfully submitted more than one article per year under this effort in refereed journals as highlighted in Sec. 3.2. We have organized two international meetings entitled "Quantum Cryptanalysis" addressing the scope of this research. Both have been approved under the umbrella of a Dagstuhl Seminar (No. 15371 and No. 17401), and one of these was picked up by *nature* [8]. Moreover, one of the PIs met each year at AFRL/RIT to report on the status of the project.

- *(Metric 4.4.1– 4.4.4)* We meet each milestone by simulating the neck pinch of a discrete geometry and integrating through the singularity using a discrete form of manifold surgery. This evolution required re-meshing based on a discrete diffeomorphism formulation based on the PI's previous research. Our new diagonalized for of the DRF equations enabled us to mirror Forman's curvature [50] and we applied our DRF technique to a real world network (RWN) of e-mail exchanges.

- *(Metric 4.5.1–4.5.4)* Our PhD student successfully defended his thesis by analyzing, for the first time, the definition of quasi-local mass developed by S-T Yau and M-T Wang. This calculation was involved, and pointed out some improvements needed in their theory. This application is being used to define a quasi-local definition of congestion in networks. This definition mirrors the Wang and Yau definition for quasi-local energy and momentum in general relativity. This future research will be conducted by S. Ray at the AFRL under his National Research Council (NRC) postdoctoral fellowship.

We met or exceeded all five metrics and milestones described above, with two exceptions:

- Integrating self-synchronization into $\alpha\eta$ appears to require pre-processing of the raw data or/and a post-processing of data transmitted through the optic channel. The defining properties of an AONT seem to rule out a preprocessing approach. For a post-processing approach, it is unclear how to integrate with the error correction for the optic channel without invalidating the security proof. As the design of our encryption scheme enables us to send only parts of the data over the optic channel and we emphasized provable security, we think that our basic error correction that goes along with the security analysis is a pragmatic workaround.

- We were only able to examine the change in curvature-based heat maps under DRF but have not finished defining and benchmarking a QLC measure related to these curvature quantities. In particular, much of our research with PhD student Shannon Ray was consumed in analyzing the Wang and Yau QLM definition. This result was necessary, and the students results lead to his degree and was successful in establishing a postdoctoral position at AFRL/RIT. He will continue this research under this NRC and apply a our results to quantum systems. The community has acknowledged that we have developed the first faithful discrete representation of Hamilton's Ricci Flow integrating through a singularity using a discrete form of manifold surgery. We used discrete re-meshing (discrete diffeomorphism) to accomplish this evolution. Exciting applications are underway both of pure mathematical foundation as well as applied complex network problems.

3.2 Publications Under this Effort

There are 7 publications in refereed journals, 1 publication in refereed conference proceedings, two Dagstuhl reports, and a (refereed) poster presentation associated to this effort; two more papers on protecting point-to-point connections are close to completion and about to be submitted. The publications are as follows:

1. Alsing, P. M., Miller, W. A. and Yau, S-T, "A realization of Thurston's geometrization: discrete Ricci flow with surgery," *Annals of Mathematical Sciences and Applications* (2018) in press ; arXiv:1709.08494.

2. Conboye, R and Miller, W. A., "Piecewise flat curvature and Ricci flow in three dimensions," *Asian J. Math.* **6**(6) (2017) 1063-1098.

3. Miller, W. A., Ray, S., Wang, M-T & Yau, S-T, "Wang and Yau's quasi-local energy for an extreme Kerr spacetime," *Class. Quantum Grav.* (2018) in press ; arXiv:1708.07532.

4. Ray, S., Miller, W. A., Alsing, P. M. & Yau, S-T, "Adiabatic isometric mapping algorithm for embedding polyhedral metrics in Euclidean 3 space," *Class. Quantum Grav.* **32**(23) (2015) 235012.

5. Alsing. P., Blair, H. A., Corne, M., Jones, G., Miller, W. A., Mischaikow, K. and Nanda, V. "Topological Signatures of Singularities in Simplicial Ricci Flow," *Axioms* **6**(3) (2017) 24.

7. Conboye, R., Miller, W. A. and Ray, S., "Distributed mean curvature on a discrete manifold for Regge calculus," *Class. Quantum Grav.* **32** (2015) 185009.

8. Kepley, S., Russo, D., Steinwandt, "Cryptanalysis of a modern rotor machine in a multicast setting," *Cryptologia* **40(6)** (2016) 515–521.

9. Grassl, M., Langenberg, B., Roetteler, M., and Steinwandt, R., "Applying Grover's algorithm to AES: quantum resource estimates," in T. Takagi, editor, *Post-Quantum Cryptography*, Lect. Notes in Comput. Sci. vol. 9606, Springer (2016) 9–43.

10. Amento, B., Grassl, M., Langenberg, B., Liu, Y.-K., Schoute, E., and Steinwandt, R., "Quantum Cryptanalysis of Block Ciphers: A Case Study," *21st Annual Conference on Quantum Information Processing*, (2018) poster.

11. Mosca, M., Roetteler, R., Sendrier, N., Steinwandt, R. (eds.), "Quantum Cryptanalysis (Dagstuhl Seminar 15371)," *Dagstuhl Reports*, **5(9)**, (2015) 1–17.

12. Mosca, M., Sendrier, N., Steinwandt, R., Svore, K. (eds.), "Quantum Cryptanalysis (Dagstuhl Seminar 17401)," *Dagstuhl Reports* , (2018) to appear.

4 RESULTS AND DISCUSSION

4.1 Security of Point-to-Point Connections

The results on point-to-point connection roughly split into

1. Resource estimates for quantum attacks, primarily focusing on the resource analysis of implementing an exhaustive key search with Grover's algorithm against various prominent block ciphers. In addition to one of the PIs, Brittanney Amento (Florida Atlantic Univ.), Markus Grassl (Max-Planck Gesellschaft, Germany), Brandon Langenberg (Florida Atlantic Univ.), Yi-Kai Liu (NIST), and Eddie Schoute (Univ. of Maryland) participated in this part of the project research. For a classical cryptanalytic result, David Russo and Shane Kepley, two students at the PIs' institution were collaboration partners.

2. The integration of classical pre- (and post-)processing into $\alpha\eta$ to establish strong provable guarantees, primarily in an information-theoretic setting without the introduction of computational assumptions. In addition to one of the PIs, two students at the PIs' institution — Hai Pham (Florida Atlantic University) and Shane Kepley (Florida Atlantic University) — as well as Adriana Súarez Corona (Universidad de Léon, Spain) were collaboration partners.

4.1.1 Resource Estimates for Quantum Attacks

In symmetric cryptography, arguably the most straightforward form of quantum cryptanalysis is to perform exhaustive key search against a block cipher, using Grover's algorithm. Asymptotically, this achieves a quadratic speedup, compared to classical exhaustive search. The straightforward interpretation would mean that if a block cipher has k bits of security against classical computers, it will have $k/2$ bits of security against quantum computers. However, this ignores a number of issues regarding the implementation of Grover's algorithm. Even leaving aside the question of fault tolerance, we need to implement the "oracle" in Grover's algorithm – it checks (a superposition of) target keys against given plaintext-ciphertext pairs. The Grover oracle is specific to the target cipher E we attack, the implementation of the Grover oracle $U_{M,E}$ finds the (unique) key K in the key space $\mathcal{K}_E$ where the predicate $f_{M,E}(K) : \mathcal{K}_E \to \{0,1\}$, defined as

$$f_{M,E}(K) = \begin{cases} 1 & \text{if } \bigwedge_{i=1}^{r} E(M_i, K) = C_i \\ 0 & \text{otherwise.} \end{cases}, \tag{3}$$

is 1. It acts on the given inputs as

$$U_{M,E}|K\rangle|-\rangle = (-1)^{f_{M,E}(K)}|K\rangle|-\rangle\,, \tag{4}$$

$$U_{M,E}|K\rangle|+\rangle = |K\rangle|+\rangle\,. \tag{5}$$

Figure 1 and Figure 2 show two different ways to implement the testing of a candidate key against a given tuple of r plaintext-ciphertext pairs in the Grover oracle. The *parallel* Grover oracle in Figure 1 computes the encryption for all plaintexts in parallel. This oracle variant requires less gates to implement and the total circuit depth is small; the required number of qubits is higher, however. The unitaries K and E implement the key expansion and message encryption of the target cipher, respectively. Alternatively, the *sequential* oracle in Figure 2 be used to reduce the total number of qubits at the cost of increasing the gate count and circuit depth.

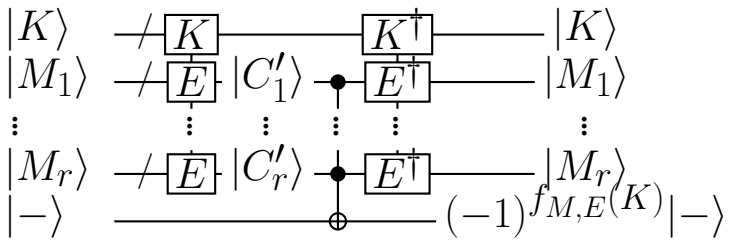

Figure 1: The parallel Grover oracle computes the encryption for all plaintexts in parallel.

Whichever option we choose, from the above figures it is clear that the structure of the specific target cipher will influence the details, and therewith the cost, of running Grover's algorithm. Table 1 (extracted from our work in [6]) gives an idea of the quite substantial differences in the cost of the quantum circuits that have been found for various block ciphers — all using a 128-bit secret key. In particular, for members of the lightweight families SIMON and SPECK a Grover attacks appears much closer to being practical than for MARS. It should be noted that the quantum circuits we identified are the first ones reported in the literature for these ciphers in this level of

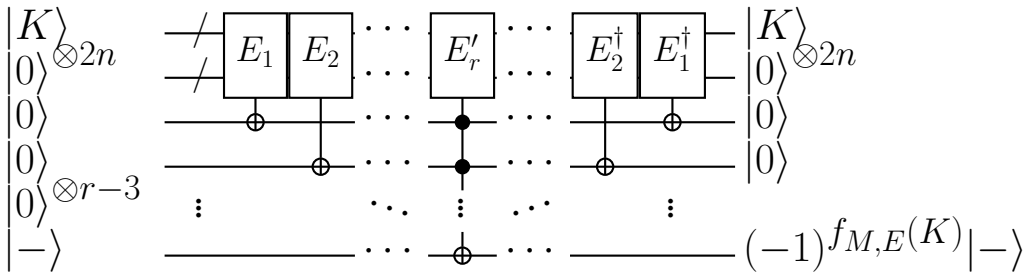

Figure 2: The sequential Grover oracle trades qubits for circuit depth.

Block cipher	Clifford	T-gates	qubits
SIMON$_{\text{par}}$(32, 4)	76,770	40,432	257
SIMON$_{\text{seq}}$(32, 4)	134,196	60,632	194
SPECK$_{\text{par}}$(32, 4)	133,858	69,328	259
SPECK$_{\text{seq}}$(32, 4)	264,900	137,282	195
SERPENT	256,314	132,608	800
MARS	$1.32 \cdot 10^8$	$9.6 \cdot 10^7$	1936
AES-128	10^6	10^6	984

Table 1: Resources for implementing various 128-bit block ciphers as a quantum circuit.

detail, and improvements can be expected. E.g., in the second Dagstuhl Seminar we organized in connection with this project, a group in the Netherlands indicated possible improvements for the gate counts in the S-box of AES. Such results will also reduce the overall gate cost of AES. For instance, Figure 3 gives a schematic overview of how we structured an AES circuit for the case of a 192-bit key, and with a more (gate) efficient S-box construction, we could obtain (gate) savings in each round – and therewith in each iteration of Grover's algorithm, i.e., local savings pay off. Note that the circuit includes the key expansion, which one may be temped to suppress in an abstract AES discussion, but as we need to encrypt plaintexts in a Grover attack, the correct round keys must be derived, and we cannot ignore the key expansion.

What makes a block cipher more resistant against a Grover-based attack? One of the answers is indicated in the above overview of a circuit for AES-192: we do have to find the round keys inside the Grover oracle. As a consequence, a complex key schedule can make the design of the Grover oracle quite complex—and at the same time, latency possibly caused by a more complex key schedule may be acceptable for a number of applications. The most fundamental issue that impacted the development effort for our quantum circuits rooted in the internals of the round functions, however: Many modern block ciphers are contain a number of linear operations as part of the round functions—AES being a prime example of such a design. For security reasons, the design also introduces some non-linear components, commonly in the form of one or several S-boxes. The type of S-boxes made quite a difference for our analysis efforts: we have to implement these "look-up tables" as a quantum circuit, which is conveniently done by first implementing a reversible circuit, and thereafter mapping reversible gates to a Clifford+T gate set, using existing decompositions [9].

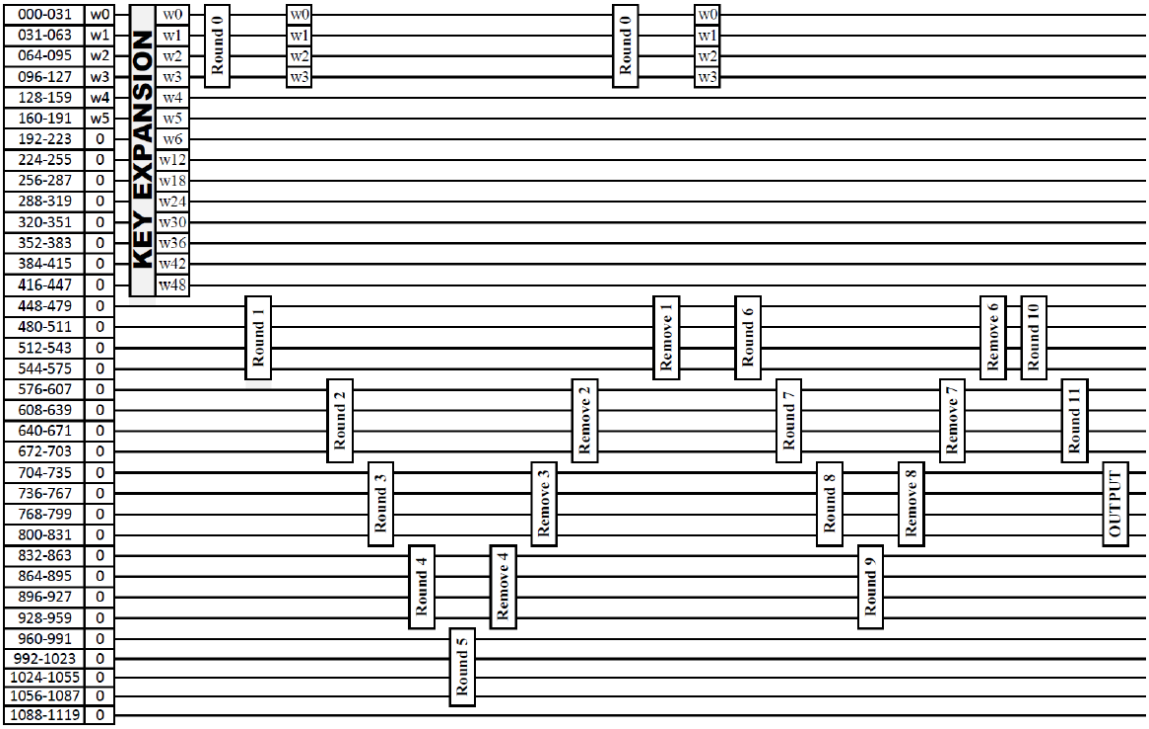

Figure 3: Structure of a quantum circuit for AES.

S-boxes that are inherently reversible and operate on a small number n of bits only can be seen as elements of the symmetric group S_n, and hence we can invoke the powerful algorithmic machinery for word problems in S_n. Such techniques are well-known from solving permutation puzzles—a permutation needs to be expressed as a *short* word in terms of given generators. In our case the generators correspond to certain elementary gates, and a word being short means we want to keep the number of gates small. Group-theortic tools could be used successfully for decomposing the S-box of AES, for instance.

Serpent is another example where a group-theoretic approach allows the construction of quite compact circuits — Figures 4 and 4 show quantum circuits for all Serpent S-boxes— depending on the round permutation being even or odd, we do need an additional qubit (ancilla):

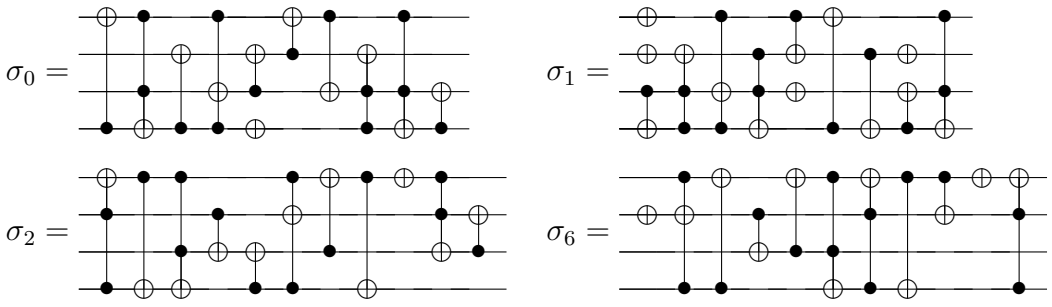

Figure 4: Quantum circuits for SERPENT's S-boxes: even permutations.

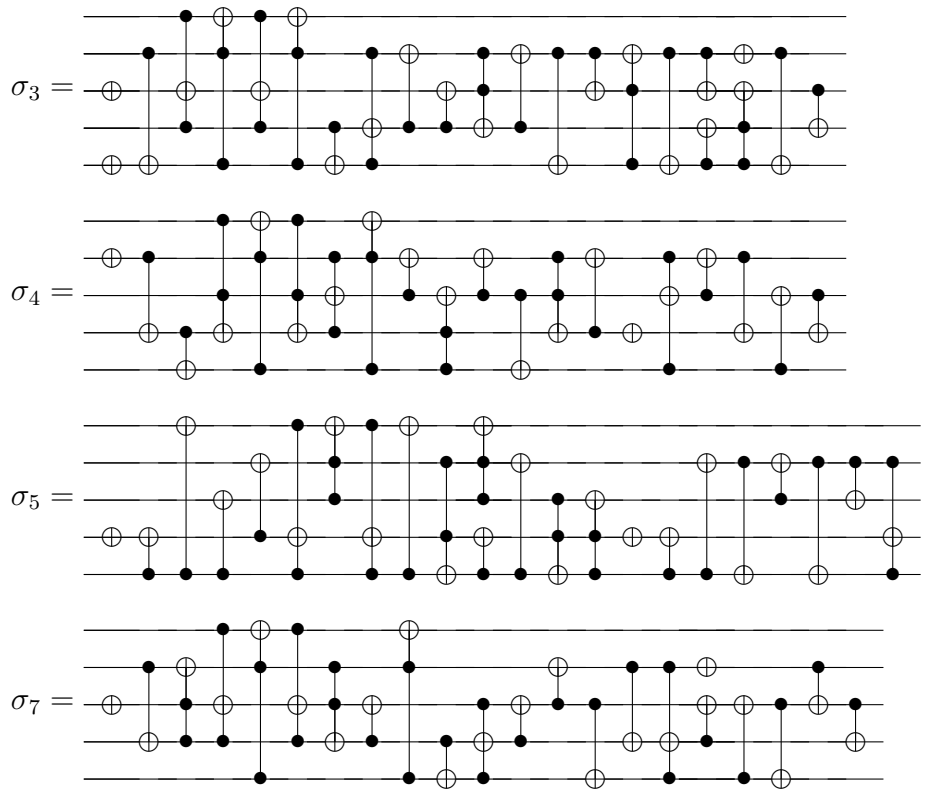

Figure 5: Quantum circuits for SERPENT's S-boxes: odd permutatons

In a sense on the opposite end of the design space is the AES finalist MARS: The MARS S-box contains 512 entries, each being a 32-bit value produced in a "pseudorandom fashion" (with a cryptographic hash function). Since no obvious algebraic structure exists to take advantage of, the most naive approach would be to implement 512 nine-fold controlled NOT gates for each of the 32 bits (i.e., checking every input bit possibility and applying the appropriate output per bit), which would result in a highly costly quantum circuit. Of course, some boolean simplification can be applied here, but we failed to find "impressive" simplifications that come from structural insight—the lack of algebraic structure appears to effectively limit the tools available. Implementing the unstructured S-box dominates the design and implementation cost of the Grover oracle for MARS. Having large "random" S-boxes appears at this point an adequate design tool to increase the complexity of a Grover-based attack.

4.1.2 Enhancing $\alpha\eta$ through the Integration of Classical Cryptographic Techniques

To be able to discuss a protocol like $\alpha\eta$ and its integration into a hybrid scheme, we use the notion of a *quantum symmetric-key encryption scheme using mesoscopic coherent states*. This is a triple of efficient algorithms as follows:

- `KeyGen`: given the security parameter, it outputs a secret key K.
- `Encryption`: given a plaintext M and a secret key K, it outputs a ciphertext C, consisting of a sequence of coherent states and a bitstring of the form

$$C = (|\psi_1\rangle, \ldots |\psi_m\rangle || c_1, \ldots, c_n)$$

- `Decryption`: given a ciphertext C and a secret key K, it outputs a plaintext M.

We allow the sequence of coherent states or the classical bit string to be empty to include both classical and purely non-classical symmetric-key encryption schemes. The key tool to preprocess data in such a way that we can make less use of the optic channel (without sacrificing security) is an AONT. In terms of the entropy function H, we can characterize an AONT as follows: Let $X_1, ..., X_s, Y_1, ..., Y_s$ be random variables taking values from the finite set X, with $|X| = v$. These $2s$ random variables define a (l, s, v)-AONT provided that the following conditions, are satisfied:

1. $H(Y_1, ..., Y_s|X_1, ..., X_s) = 0$,
2. $H(X_1, ..., X_s|Y_1, ..., Y_s) = 0$
3. For all $\mathcal{X} \subseteq \{X_1, ..., X_s\}$ with $|\mathcal{X}| = l$, and for all $\mathcal{Y} \subseteq \{Y_1, ..., Y_s\}$ with $|\mathcal{Y}| = l$, it holds that
$$H(\mathcal{X}|\{Y_1, ..., Y_s\}\backslash\mathcal{Y}) = H(\mathcal{X})$$

For the purpose of this project, we are only interested in AONTs that can be constructed efficiently, and a result of Stinson [10] can be used to derive efficient constructions of *linear* AONTs when X is a finite field. Regrettably, Stinson's result does not apply when we care about an analysis at the bit-level. Being able to protect the secrecy of individual bits is a cryptographic necessity, however, and so we introduced a notion of restricted AONT, which is less versatile than an AONT, but the restriction imposed does not matter for our application. Essentially, we restricted the positions of the unknown output-values in the definition of an AONT. In our context, this will mean that we fix which bits will be transmitted by means of the optic channel with an $\alpha\eta$-type protocol, and which bits of the restricted AONT output can be exposed on a classical transmission channel. The simplest case of a restricted AONT is a 1-*restriced* AONT: Let $X_1, ..., X_s, Y_1, ..., Y_s$ be random variables taking on values in the finite set X. These $2s$ random variables define a 1-restricted AONT provided that the following conditions are satisfied:

1. $H(Y_1, ..., Y_s|X_1, ..., X_s) = 0$
2. $H(X_1, ..., X_s|Y_1, ..., Y_s) = 0$
3. For all i such that $1 \leq i \leq s$, $H(X_i|Y_2, ..., Y_s) = H(X_i)$.

There is no harm for us, in imposing restrictions on our position choices in advance, or keeping this choice secret. An AONT has no secret key. In fact, the restricted AONTs we are interested in come from highly structured binary matrices. Namely, the binary matrices we are interested in, have the following form, and applying a restricted AONTs boils down to simple matrix-by-vector multiplication:

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{bmatrix}$$

Schematically, our protocol design is summarized in Figure 6. One topic that so far did not receive sufficient attention in the literature is the security impact of error correction on the optic channel,

which is clearly needed, if we target high-speed applications and take realistic error rates (cf. [11]) into account. In order to be able to establish a provable result, we settled for an admittedly very simple error correction approach — a binary repetition code. As this affects only the part of the preprocessed message that is sent over the optic channel — which can be small — this seems completely sufficient. And with this construction we can indeed provide information-theoretic security bounds on the security of the resulting encryption scheme. As neither the restricted AONT nor the error correction rely on computational assumptions, the security model and guarantee are theoretically quite "clean."

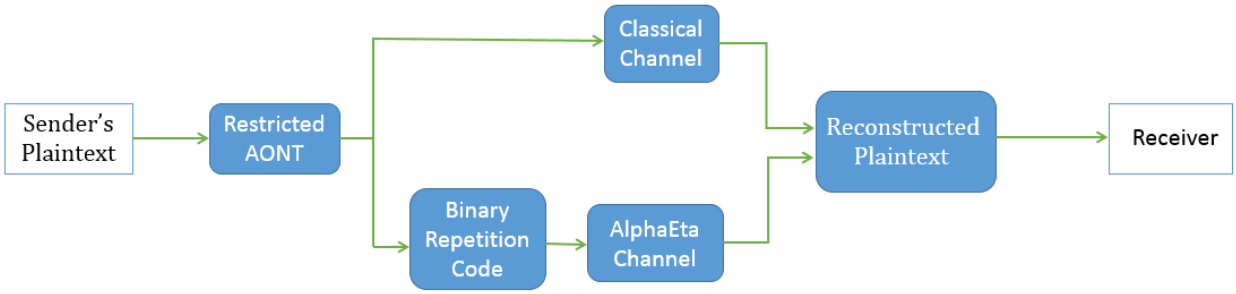

Figure 6: Schematic overview of the hybrid protocol.

Of course, in this type of model side-channels are not taken into consideration. Main restriction is the (not very surprising) need for a certain amount of entropy in the raw payload to be transmitted. Leaving the information-theoretic setting, we anticipate that the payload would be preprocessed with a classical high-speed AEAD anyway. Concatenating this with our hybrid scheme results in a situation where the adversary even lacks the ciphertext to mount an attack against the AEAD. Another (information-theoretic) feature of our design is that it comes inherently with a forward secrecy guarantee – assuming suitable restrictions on the (experimental) abilities of the adversary, we could established that past input bits remain protected even after comprise of the secret key. Of course, for future transmissions no more guarantees can be provided then.

Downside of our scheme is that the restricted AONT prevents us from benefiting from potentially available self-synchronization guarantees of the classical AEAD solution. However, in view of the limited bandwidth need for the optic channel in our design, this appears a price worth paying. With the new construction we can make extensive use of a classic channel and still, provably, preserve $\alpha\eta$ advantages.

4.2 Global Analysis of Complex Networks

A discrete RF (DRF) approach for three and higher dimensions, referred to as Simplicial Ricci Flow (SRF), has been introduced recently and is founded on Regge calculus [26, 27, 28], as well as complementary work in this direction by [29, 30, 31, 32, 50]. The equations of SRF are similar to their continuum counterpart and were shown for this model to convergent. Recently, the Rc_e tensor was reconstructed on each edge e of a lattice geometry [35]. Here they defined (Definition 5.3) a volume associated to edge $e = \overline{v_1 v_2}$ that was capped at each of the two bounding endpoints v_1 and v_2. However, in this work we extended the volume associated to the edge e to include the union of the two Voronoi volumes associated to bounding vertices of the edge,

$$V_e = V_{v_1} \cup V_{v_2}. \tag{6}$$

In so doing, we avoided the need to artificially cap the ends of the volume. The formulae for the Ricci curvature (Eq. 1.3) of the edge in [35] is identical for this extended volume, it just includes more edges in the summation. Even though both volumes gave essentially equivalent neck pinching dynamics, we choose the extended volume as it adheres closely to the approach by Forman [50]. These new DRF equations form a diagonalized set of first-order autonomous nonlinear differential equations in time. There is one equation per edge in the lattice geometry,

$$\frac{1}{\ell_e}\frac{d\ell_e}{dt} = -Rc_e = -K_e + \frac{1}{2}R_e. \tag{7}$$

In this DRF equation [35] we use an alternative but equally valid vertex-weighted expression:

1. K_e is the sectional curvature of edge $\ell_e = \overline{v_1 v_2}$ and is given in terms of the sum over all the edges, ℓ_{e_j} that share a common vertex (v_1 and/or v_2) with edge ℓ_e,

$$K_e = \frac{1}{V_e}\sum_{e_{v_1}, e_{v_2} \sim e}\left(\frac{\cos^2(\theta_{e_{v_1}})\epsilon_{e_{v_1}}}{A_{e_{v_1}}}V_{e_{v_1}} + \frac{\cos^2(\theta_{e_{v_2}})\epsilon_{e_{v_2}}}{A_{e_{v_2}}}V_{e_{v_2}}\right).$$

   The data structure for this sectional curvature is illustrated in (Fig. 7). Included in this data structure are all the edges that share either vertex v_1 or v_2 or both. This data structure is common for both the discrete Ricci flow tensor Rc_{DRF} used here as well as the Forman graph Ricci curvature Rc_F for an edge e in a graph. It is expressed in terms of the Voronoi areas A_j dual to the edges ℓ_j, the sum of the dual Voronoi 3-volumes of the vertices bounding edge e,

$$V_e = V_{v_1} + V_{v_2},$$

   the deficit areas ϵ_j of these edges used in Regge calculus [36], as well as the angle θ_j between edge ℓ_e and ℓ_j. Here, $V_{e_{v1}}$ is the fraction of the dual Voronoi volume, V_{v1} associated with edge e_{v1}. These are explicitly defined for this model in [37, 39, 40]. Additionally,

2. R_e is the scalar curvature associated to edge ℓ_e, and it is expressed in terms of the average of the scalar curvatures at each of the endpoints of edge $\ell_e = \overline{v_1 v_2}$,

$$R_e = \frac{1}{2}\left(R_{v_1} + R_{v_2}\right).$$

The vertex-based scalar curvatures were introduced earlier in Regge calculus, and is a certain weighted sum of the curvatures of the edges meeting a given vertex [37],

$$R_v = \frac{1}{V_v}\sum_{e \sim v}\ell_e \epsilon_e.$$

Here V_v is the dual volume associated with vertex v, and ℓ_e is the length of the edge emanating from vertex v.

Our research under this program explored the behavior of these new diagonalized DRF equations in 3-dimensions for a geometry with axial symmetry, and to examined the development of a Type-1 neck pinch singularity through the singularity using manifold surgery techniques. Thus providing the first piecewise linear numerical realization of Thurston's geometrization using manifold surgery.

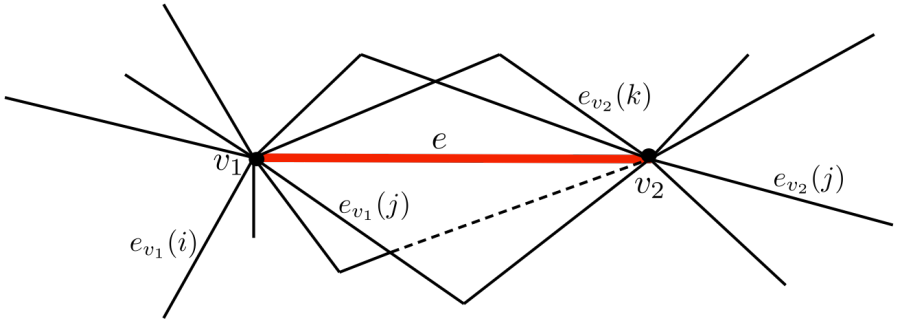

Figure 7: The data structure of an edge ($e = \overline{v_1 v_2}$) used in our definition of the Forman-Ricci tensor.

4.2.1 The 3-Dimensional Neck Pinch Model

We use the analysis of Angenent and Knopf on the Type-1 singularity analysis of the continuum RF equations as a foundation of this work [38]. They carefully analyzed a class of axisymmetric double-lobed shaped geometries with mirror symmetry about the plane of the neck as illustrated in the top of Fig. 8. In 3D the continuum cross-sections are 3-spheres and not circles, and in our discrete model the cross sections are icosahedrons and not hexagons. The 3D cells are triangle-based frustum blocks as opposed to the trapezoids depicted in the bottom of the figure. Here the variable a_c measures the proper distance from the equator, and s is the length of the icosahedron edges.The symmetry of this geometry allows us to suppress one of the three dimensions for visualization purposes. In [38] RF was applied to a warped product metric on $I \times S^2$ having the form,

$$g = \underbrace{\varphi(z)^2 dz^2}_{da^2} + \rho(z)^2 g_{can} \tag{8}$$

$$= da^2 + \rho(a)^2 g_{can}. \tag{9}$$

Here, $I \in \mathbb{R}$ is an open interval,

$$g_{can} = d\theta^2 + \sin^2\theta d\phi^2, \tag{10}$$

is the metric of the unit 2-sphere,

$$a(z) = \int_0^z \varphi(z) dz, \tag{11}$$

is the geodesic axial distance away from the waist, and $\rho(a)$ is the radial profile of the mirror-symmetric geometry, i.e. $s = \rho(a)$ is the radius of the cross-sectional 2-sphere at axial distance a from the waist. Angenent and Knopf proved that the RF evolution for such a geometry has the following properties:

1. If the scalar curvature is everywhere positive, $R \geq 0$, then the radius of the waist ($s_{min} = \rho(0)$) is bounded, $(T - t) \leq s_{min}^2 \leq 2(T - t)$, where T is the finite time at which a neck pinch occurs.

2. As a consequence, the neck pinch singularity occurs at or before $T = s_{min}^2$.

3. The heights of the two lobes are bounded from below and, under suitable conditions, the neck will pinch off before the lobes will collapse.

4. The neck approaches a cylindrical-type singularity.

We demonstrated in our earlier work that the SRF equations, for a sufficiently pinched radial profile, reproduced the neck pinch singularity in finite time, and that the SRF evolutions agree with a finite-difference solution of the continuum RF equations for the same profile [39, 40]. However, in our previous analysis we were unable to remove the singularity by manifold surgery and so unable to integrate through the singularity and reproduce the direct product of two collapsing 3-spheres. Furthermore the equations used previously, though proven to converge to the continuum RF equations, form a sparsely-coupled set of autonomous nonlinear first-order differential equations that proved numerically difficult and time consuming to solve.

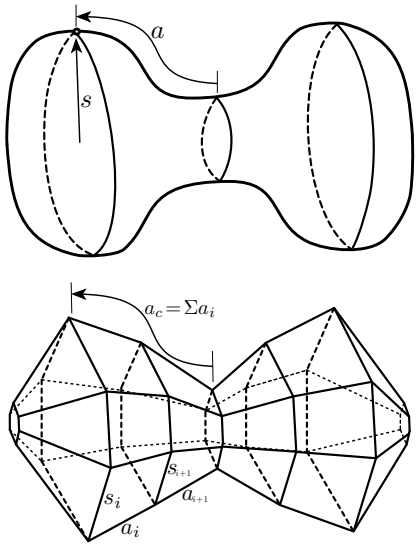

Figure 8: A two dimensional representation of the 3D neck pinch geometry of Angenent and Knopf (continuum on top, and discrete on bottom).

The discrete model reported here is a piecewise linear (PL) approximation to the double-lobed geometry (e.g. the S^2 cross sections are modeled by icosahedra, and adjacent faces of the icosahedra are connected to each other via frustum blocks) as illustrated in Fig. 9 The lattice is composed of triangle-based frustum blocks, and the dual lattice is composed of pentagonal-based frustum blocks. The expressions for the sectional, scalar, and Ricci curvature uses the dual lattice with its dodecahedral cross sections. This lattice is described more fully in [26]. Our simulation used 80 cross-sectional icosahedra across the double-lobed profile. We also relaxed the condition of mirror symmetry about the throat and considered asymmetric geometries. This work represents the first non-trivial numerical solution of the new DRF equations, and it is the first DRF integration through a Type-1 singularity via manifold surgery of which we are aware. The results are illustrated in Fig. 10. We use axial symmetry of our model to suppress one dimension and the resulting

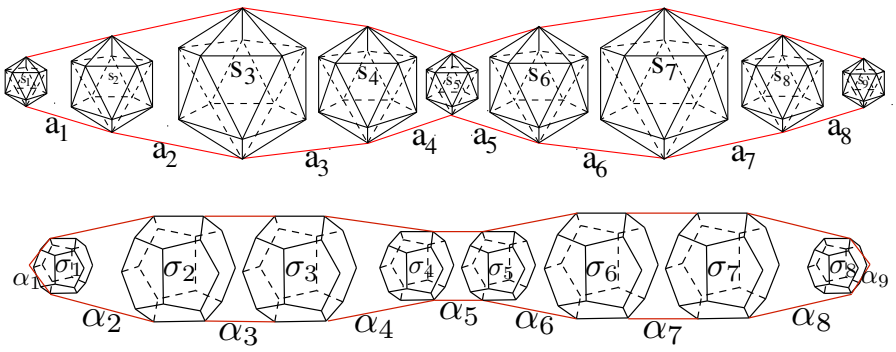

Figure 9: An illustration of the icosahedron neck pinch geometry for nine cross-sectional icosahedra (top), and its dual dodecahedral lattice (bottom).

two-lobed geometry can be visualized in Euclidean 3-space (our evolution was fortunately isometrically embeddable in R^3). The middle 3'rd and 4'th figure occur at the same time ($t = 183.0$) in the evolution. They illustrate the explicit manifold surgery, where the spherical caps (two icosahedrons)are placed on the ends of the left and right lobes. This is the first numerical illustration of Thurston's geometrization procedure that we are aware of. This surface has 3438 edges, 1580 triangle-based frustum blocks and 960 vertices, although symmetry reduces the number of edges to 80 icosahedral $\{s_i\}$ edges and 79 axial $\{a_i\}$ edges. The illustrative simulation presented here involves the solution of a diagonal set of 159 autonomous nonlinear first-order differential equations. We evolved the left and right lobes for 1682 and 2133 time steps, respectively. We used a time step $\Delta t = 0.25$. There is no longer the need for matrix inversion at each evolution step.

In the next section we describe the initial profile used and the numerical results obtained.

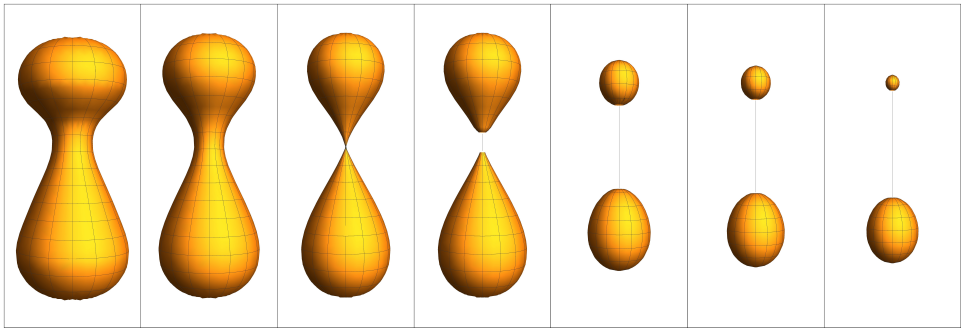

Figure 10: The RF of a lopsided neck pinch geometry through the Type-1 singularity using surgery and yielding the geometry as a direct product of two 3-spheres.

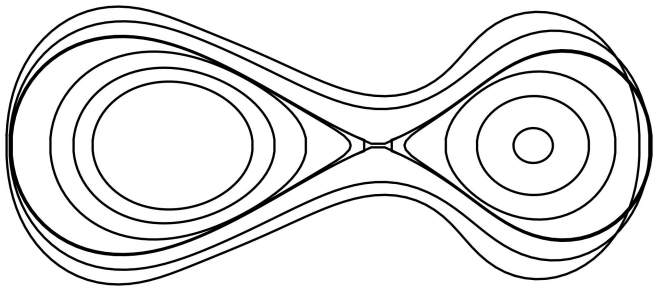

Figure 11: A 2-dimensional cross section of a lopsided neck pinch geometry evolving under RF through the Type-1 singularity.

4.2.2 DRF with Surgery: A Numerical Realization of Thurston's Geometrization for a Neck Pinch Geometry.

We evolved a sufficiently pinched axisymmetric 3-geometry which was given the initial ($t = 0$) radial profile,

$$s_i = 105.15 \left(1 - 0.2\, e^{\left(\frac{\xi_i + .4}{0.4}\right)^2} - 0.05\, e^{\left(\frac{\xi_i + 0.6}{0.3}\right)^2} \cos(\xi_i) - 0.7 \cos(\xi_i)^4 \right),\ \forall i \in \{1, ..., n\}, \quad (12)$$

and axial segments,

$$a_i = 100\ \sin(\Delta\xi),\ \forall i \in \{1, 2, ..., n-1\}, \quad (13)$$

where $\xi_i = (n-2i+1)/2$, $\Delta\xi = \pi/(n+1)$, and there are $n = 80$ icosahedral cross-sections. Fig. 10 shows the the initial profile of the lobed geometry in the rectangle to the left along with six other snapshots taken later during the evolution. This initial double-lobed geometry is also illustrated in Fig. 11 and is the outermost curve in the planar embedding. We evolve this surface by numerically solving Eq. 7. This geometry evolved to a pinch (third geometry from the left in Fig. 10) at $t = 183.0$. We evolved the equations using a fourth-order Runge-Kutta code with $\Delta t = 0.25$. At every 50 steps in this evolution we remesh the surface using a cubic spline interpolation. This remeshing was necessary to keep the circumcenter inside each frustum block (as described in [39]). Near the singularity $t = 183$ we removed the pinch by manifold surgery yielding the two lobes exhibited in Fig. 11 using the following 4-step procedure:

1. we remove the axial edge a_{45} where the geometry pinched yielding a disconnected left and right lobed geometry each with R^3 topology (the right and left boundaries were removed; respectively);

2. we capped the left and right lobes by gluing an icosahedra to these open ends with edge length s_{45} and s_{46} thus forming two disconnected 3-dimensional ovoids;

3. we remeshed each of the 3-dimensional ovoids using a cubic spline;

4. finally, we continued evolving using the DRF equations for both of the 3-dimensional ovoids.

Here, Surgery yields two disconnected 3D ovoids and each becomes spherical under the RF evolution. The resulting geometry is a direct product of two 3-spheres. As the lobed geometry collapses

a pinch occurs at t= 183. At this point we remove the axial edges at the pinch and cap each end of the left and right lobe with a new icosahedra. These two surfaces (pre and post surgery) are the 3rd and 4th layers inside the initial surface. After surgery, we remesh both the left and right 3-dimensional ovoids using cubic spline interpolation. This is, to our knowledge, the first numerical realization for PL manifolds of Thurston's geometrization procedure. This particular surface has 3348 edges, 1580 triangle-based frustum blocks and 960 vertices, although symmetry reduces the number of edges to 80 icosahedral $\{s_i\}$ edges and 79 axial $\{a_i\}$ edges.

A more sophisticated surgery procedure that we illustrate in Fig. 12 was implemented. This involved reassigning the values to two of the s variables and two of the a values. This procedure offers no essential advantage over the simpler procedure consisting of just capping the surgery with an icosahedron and remeshing. Here we replace the last three s variables and two a variables with their spherical cap values. Because we found that this more time-consuming and sophisticated approach yields the same results, we chose to use the more austere procedure enumerated above. We evolved these two lobes separately using the Eq. 7. Under this flow the curvature uniformized and the lobes each evolved toward a collapsing 3-sphere geometry as shown in the figure. We reproduced expected results with the new DRF equations as shown in Fig. 10 and Fig. 11. In other words, the initial geometry evolved toward a direct product of two constant curvature Thurston geometries, and in particular, as a direct product of two 3-spheres.

This numerical example demonstrates our ability to integrate through a singularity and realize the Thurston decomposition. Our current approach is numerically more efficient than our earlier formulations.

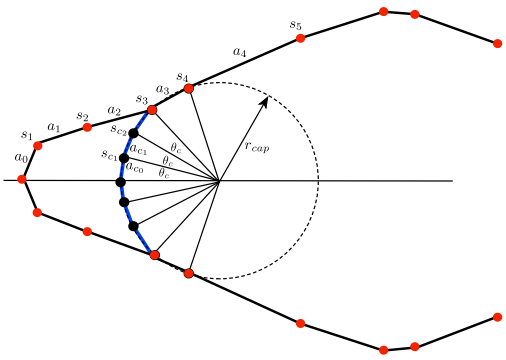

Figure 12: After the manifold surgery the lobe was closed using a spherical cap with proper matching conditions as illustrated in this figure.

4.2.3 From Piecewise Linear Curvature to Graph Curvature

While we focused our research on the discrete Ricci flow of a PL geometry and manifold surgery, we applied our formulation based on Forman's curvature construction to more general structures, e.g. graphs. It is our focus to explore the properties of graph curvature flow and determine its utility in characterizing the graph structure, or in its ability to identify and diffuse interesting curvature regions in the graph. To this end, there is considerable interest and pioneering work in applying the Ricci flow techniques to characterize and identify change in dynamic small-world spatial networks [41, 42]. Positive curvature networks stabilize, while negative hyperbolic curved networks expand. The key to these approaches is a measure of the Ricci curvature introduced by Forman [50]. We

identified a striking, but intuitive, relationship between the Forman Ricci curvature Rc_F on graphs and our formulation of the discrete Ricci tensor $Rc_{_{DRF}}$ [34, 35],

$$Rc_F = \frac{1}{2}\left(\frac{\omega(v_1)}{\omega(e)} + \frac{\omega(v_2)}{\omega(e)}\right) - \sum_{e_{v_1}, e_{v_2} \sim e} \frac{1}{2}\left(\frac{\omega(v_1)}{\sqrt{\omega(e)\omega(e_{v_1})}} + \frac{\omega(v_2)}{\sqrt{\omega(e)\omega(e_{v_2})}}\right), \tag{14}$$

$$Rc_{_{DRF}} = \frac{1}{2}\left(\frac{R_{v_1} + R_{v_2}}{2}\right) - \sum_{e_{v_1}, e_{v_2} \sim e} \frac{1}{2}\left(\frac{\cos^2(\theta_{e_{v1}})\epsilon_{e_{v_1}}}{A_{e_{v_1}}} + \frac{\cos^2(\theta_{e_{v2}})\epsilon_{e_{v_2}}}{A_{e_{v_2}}}\right) \tag{15}$$

Here, e is the edge under consideration between two nodes v_1 and v_2, the edges sharing node v_1 are denoted by e_{v_i} and are each weighted by an appropriate weighting function $\omega(e_{v_i}) \in [0, 1]$ (with $i = \{1, 2\}$), and $\omega(v_i) \in [0, 1]$ is the weighting function for node v_i. The data structure as shown in Fig.7 is identical for both the discrete Ricci tensor and the Forman curvature on graphs. The comparison of these two curvatures for a given simplicial network, e.g. the 600-cell polytope, could sharpen the definition of the vertex and edge weighting function for the Forman curvature. This suggests the following correspondence:

$$\omega(v_j) \longleftrightarrow \cos^2\left(\theta_{e_j}\right)\epsilon_{e_j} \tag{16}$$

$$\sqrt{\omega(e_j)\omega(e)} \longleftrightarrow A_{e_j} \tag{17}$$

We believe this may lead to discoveries characterizing complex networks and continued work resulting from this program is already underway [43].

4.2.4 An Example Application to a Real World Network: Curvature Heat Maps

W demonstratde the calculation of the Forman Ricci curvature for a very small portion of the an e-mail network. In this example we examine seven e-mail exchangers over a multi-year period. We excised a small portion of the e-mail data base. The details are not important as we are just using this to illustrate the graph Ricci curvature technique introduced in this report with actual data. The graph shown in Fig. 13 was constructed with nodes (colored circles of different radii) are people and links (lines of varying thickness) between nodes indicate that two people were on a common e-mail thread. The size of a node shows the number of e-mail threads in which a person participated. The thickness of a link denotes the number of shared e-mail threads between two people. Each node is algorithmically assigned to a community (a group with a disproportionately large number of links among them), which is shown by node color.

For my purpose, the seven vertices of the graph that we investigated are be labeled as follows: (v_1) node weight of 24; (v_2) node weight of 19; (v_3) node weight of 15; (v_4) node weight of 8; (v_5) node weight of 7; (v_6) node weight of 12; and finally (v_7) node weight of 4.

The edge weighting matrix of the e-mail threads is a symmetric matrix, and its entries is determined by the number of shared e-mail threads, in particular we find

$$\omega\left(e\right) = \mathbb{1} - \frac{1}{5}\begin{pmatrix} 0 & 4 & 4 & 1 & 1 & 5 & 2 \\ 4 & 0 & 5 & 2 & 2 & 3 & 2 \\ 4 & 5 & 0 & 5 & 2 & 3 & 2 \\ 1 & 2 & 5 & 0 & 1 & 1 & 1 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 5 & 3 & 3 & 1 & 0. & 0 & 0 \\ 2 & 2 & 2 & 1 & 0 & 0 & 0 \end{pmatrix}. \tag{18}$$

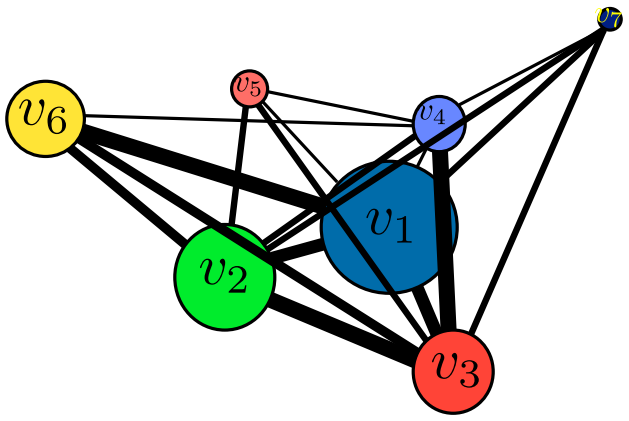

Figure 13: *Seven-node e-mail sub-network based on seven e-mail exchangers collected over several years.*

The curvature map can be calculated using Eq. 14 with the node weighting

$$\omega(v) = \begin{pmatrix} 1.00 \\ 0.79 \\ 0.63 \\ 0.33 \\ 0.29 \\ 0.50 \\ 0.17 \end{pmatrix}. \tag{19}$$

.

There are 21 edges in this graph, e.g. $e_1 = \overline{v_1 v_2}$. We used Eq. 14 to construct the following curvature map for this graph.

4.2.5 Wang and Yau's Quasi Local Mass

This section summarizes our work with PhD student Shannon Ray on exploring the definition of quasi-local mass in a gravitational field [49]. The local value for the energy density of a gravitational field is zero since the Einstein tensor is divergenceless and it is proportional to the stress energy. This is true even in the strongest gravitational fields and fluxes in the universe. In order to provide a physical and meaningful definition of the effective energy-density of a pure gravitational field, one must define it over a non-zero volume; hence the name quasi-local energy or quasi-local mass. Early definitions have been flawed and had led to the most recent definition by S-T Yau and M-T Wang [53]. Under this project we pushed their theory by examining their definition of quasi-local mass of a ball of radius $R > M$ surrounding an extreme rotating Kerr black hole of mass M [49]. This is of interest to this project because it opens a new and novel approach to define a quasi-local congestion measure of a RWN; especially given our curvature measures and the established relation between curvature and load balance in a network.

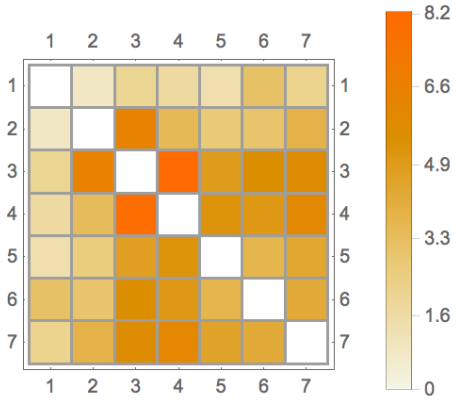

Figure 14: *Modified Forman Ricci curvature map (Eq. 14) for the graph illustrated in Fig. 13.*

The key to defining such a quasi-local quantity is to be able to subtract a ground-state energy. This was originally done by Brown and York by embedding the surface of the non-zero volume in flat Euclidean space; however not all 2-surfaces are embeddable in Euclidean space and it gives non-zero values for some flat spacetimes. Wang and Yau generalized this to optimal embeddings of the surface into flat Minkowski spacetime, and providing physically meaningful junction conditions between their embedding and the surface in the original curved spacetime.

In our work we explored the landscape of the Wang-Yau quasi-local energy for balls surrounding an extremely rotating black hole. Below a certain critical radius the constant radius spheres surrounding the Kerr black hole can no longer be embedded into Euclidean space, but can be embedded isometrically into Minkowski spacetime as shown in Fig. 15. Here, the image to the right is an isometric embedding of the spherical Boyer-Lindquist surface for $R = 3/2M$ into Minkowski spacetime. This surface is not isometrically embeddable into Euclidean 3-space, $\boldsymbol{R}^3$. The equatorial rim is embeddable in Euclidean 3-space; however, the two polar caps are isometrically embeddable in $\boldsymbol{R}^{2,1}$. The graph on the left shows a plot of the isometric embedding into $\boldsymbol{R}^{3,1}$ for a $\phi = 0$ cross-section (one dimension suppressed). In regions below the critical radius the

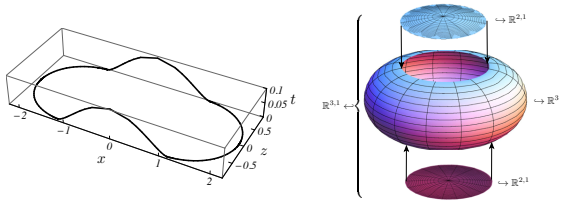

Figure 15: *Isometric embedding of the spherical Boyer-Lindquist surface for $R = 3/2M$ into Minkowski spacetime.*

Wang-Yau definition ruled out these surfaces, and they returned an imaginary value for the quasi-

local mass (Fig. 16. This figure is a contour plot of quasi-local energy as a function of the two Fourier coefficients with a_1 on the x-axis and a_3 on the y-axis. The line connecting the points indicates the path taken by the simplex method when optimizing the functional. The surfaces shown at the bottom of the figure are the convex shadows in $\mathbb{R}^3$ at three points along the minimization path. The surface to the lower right represents our initial guess, the surface in the lower left represents the global minimum, and the central surface is a surface with an intermediate value of E. Our numerical results are consistent with the global minimum occurring on the boundary of admissible solutions, i.e. on the boundary of the color saturated gap in the middle of the contour plot where the energy has an imaginary component $Im(E) > 0$.This suggests that we need to further modify their definition and provide a quasi-local mass that has physical significance. We are currently working on this problem and its extension to graph congestion.

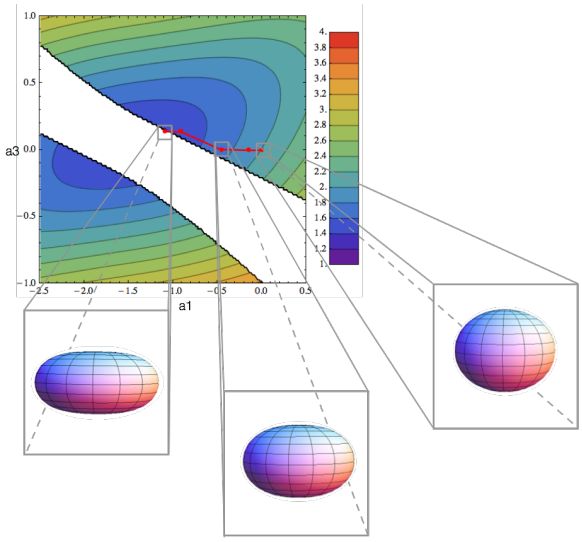

Figure 16: *Landscape of the Wang-Yau quasi-local energy for a sphere around a Kerr black hole in the space of the first two Fourier coefficients* a_1 *and* a_3.

5 CONCLUSIONS

Over the course of this project, we have been able to substantially advance the quantitative analysis of quantum attacks against point-to-point connections – a workshop we organized was picked up by *nature*, our work on AES was used by NIST to inform an ongoing standardization process, follow-up research has been initiated, and in the second international Quantum Cryptanalysis workshop we organized in connection with this project, there was not enough space to admit everyone interested in attending. With our findings, we can now confidently choose block ciphers that offer meaningful resistance against Grover's algorithm without sacrificing performance. Our work clearly shows that key length alone is too coarse a measure to estimate the cost of a quantum attack, but suitable S-boxes and key schedules are potent design tools to complicate a key search with a quantum computer.

At this point, the more urgent questions for understanding quantum attacks are on the asymmetric side – e.g., the open research literature offers very limited help in working out a complete

quantum attack against a standardized signature scheme using elliptic curves. Even writing down a specific circuit implementing Shor's algorithm against a realistic RSA-parameter is far from straightforward, as details of the arithmetic need to be worked out as a quantum circuit. Finally, mapping a logical quantum circuit onto quantum hardware also requires (at least for today's cryptanalytic applications) quantum error correction, and the details of this step – and the resulting cost overhead – are still not very well understood.

On the design side, we have shown that $\alpha\eta$ can greatly benefit from adding classical pre- (and post-)processing. We showed that information-theoretic guarantees can be established that enable a more reduced use of the optic channel in favor of using a more exposed classical channel. Even taking error correction into account, strong security guarantees can be established, including a situation where the secret key eventually gets exposed.

It seems plausible that the set of DRF equations will have an equally rich spectrum of application as does its 2-dimensional counterpart known as combinatorial RF [44]. We therefore are motivated to explore the DRF in higher dimensions so that it can be used in the analysis of topology and geometry, both numerically and analytically, to bound Ricci curvature in discrete geometries and to analyze and better handle higher–dimensional RF singularities [45, 46]. The topological taxonomy afforded by RF is richer in 3D than in 2D. In particular, the uniformization theorem says that any 2–geometry will evolve under RF to a constant curvature sphere, plane or hyperboloid, while in 3–dimensions the curvature and surface will diffuse into a connected sum of eight distinct prime manifolds [20]. We ask is there a similar uniformization/geometrization theorem for 2D/3D spatial networks?

We plan on using this to further define quasi-local congestion on an embedded network geometry. We will borrow the theoretical construction of Wang and Yau in their definition of quasi-local mass in general relativity and apply this to the simplicial geometry of an embedded network. Needed in this construction is a Hamiltonian for the embedded network. Guiding this research is the widely accepted conjecture that curvature is a measure of congestion and load balance in networks. While we are just at the beginning of this research, we believe this holds promise to address one of the deepest questions in complex networks: "What is the normal state of the network?"

The work presented here on global analysis of complex networks proposes a novel approach to RWN characterization. It gives us a natural path for transitioning this research beyond this project to the following milestones:

1. Explore more fully the use of persistent homology (PH) to identify singularity formation.

2. Develop a fully-efficient algorithm using SRF with surgery and diffeomorphism to decompose simplicial 3-manifolds into a finite connected sum of their prime components.

3. Develop quasi-local congestion and use this in PH as a filtration parameter to identify, monitor and ameliorate abnormal states of a complex network.

4. Apply SRF to 3-geometries with boundary for applications extending domain of combinatorial RF on 2-surfaces.

Acknowledgements

Contractor acknowledges Government's support in the publication of this report. We acknowledge all co-authors and colleagues that contributed to this research. This material is based upon work

funded by AFRL, under AFRL Contract No. FA8750-15-2-0047. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of AFRL.

6 LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AFRL	Air Force Research Laboratory
AONT	All-Or-Nothing-Transform
DRF	Discrete Ricci Flow
CRF	Combinatorial Ricci Flow
FAU	Florida Atlantic University
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PH	Persistent Homology
PI	Principle Investigator
PL	Piecewise Linear
QLC	Quasi-Local Congestion
QLM	Quasi-Local Mass
RC	Regge Calculus
RWN	Real World Networks
RF	Ricci Flow
RI	Information Directorate
RITC	Emerging Computing Technology
SRF	Simplicial Ricci Flow
US	United States

7 REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* **26(5)** (1997),1484–1509.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (STOC 1996)* (1996) 212–219.

[3] NIST, Information Technology Laboratory, Security Rsource Center, *Post-Quantum Cryptography Standardization*, `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization` (2017).

[4] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grovers algorithm to AES: quantum resource estimates," in T. Takagi, editor, *Post-Quantum Cryptography*, Lect. Notes in Comput. Sci. vol. 9606, Springer (2016) 9–43.

[5] National Institute of Standards and Technology, *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*, `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf` (2016).

[6] B. Amento, M. Grassl, B. Langenberg, Y.-K. Liu, E. Schoute, and R. Steinwandt, "Quantum Cryptanalysis of Block Ciphers: A Case Study," *21st Annual Conference on Quantum Information Processing*, (2018) poster.

[7] H. P. Yuen, P. Kumar, E. Corndorf, and R. Nair, "Security of Y-00 and similar quantum cryptographic protocols,", arXiv:quant-ph/0407067 (2004).

[8] C. Cesare, "Online security braces for quantum revolution," *nature* **525(7568)** (2015), 167–168.

[9] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems , **32(6)** (2013) 818–830.

[10] D. R. Stinson, "Something about all or nothing (transforms)," Designs, Codes and Cryptography **22(2)** (2001), 133–138.

[11] G. A. Barbosa and J. van de Graaf, "Untappable communication channels over optical fibers from quantum-optical noise," IACR Cryptology ePrint Archive **2014:146** (2014)

[12] R. Hamilton, "Three-manifolds with positive Ricci curvature," *J. Diff. Geom* **17** (1982), 255-306.

[13] H-D. Cao, B. Chow, S-C Chu & S-T Yau, eds., *Collected Papers on Ricci Flow* in Series in Geometry and Topology, Volume 37 (International Press; Somerville, MA; 2003).

[14] B. Chow & D. Knopf, *The Ricci Flow: An Introduction*, Mathematical Surveys and Monographs, Volume 110 (American Mathematical Society; Providence, RI; 2004).

[15] B Chow, P. Lu & L. Ni, *Hamilton's Ricci Flow*, Graduate Studies in Mathematics, Volume 77 (American Mathematical Society; Providence, RI; 2006).

[16] B. Chow, S-C Chu, D. Glickenstein, C. Guenther, J. Isenberg, T. Ivey, D. Knopf, P. Lu, F. Luo & L. Ni, *The Ricci Flow: Techniques and Applications, Part 1: Geometric Aspects*, Mathematical Surveys and Monographs, Volume 135 (American Mathematical Society; Providence, RI; 2007).

[17] X. Yu, X. Yin, W. Han, J. Gao & X. Gu, "Scalable routing in 3D high genus sensor networks using graph embedding," *INFOCOM 2012*: 2681-2685; Y. Wang, J. Shi, X. Yin, X. Gu, T. F. Chan, S-T Yau, A. W. Toga & P. M. Thompson, "Brain surface conformal parameterization with the Ricci flow," *IEEE Trans. Med. Imaging* **31**(2) (2012) 251-264. X. Gu, F. Luo & S-T Yau, "Fundamentals of computational conformal geometry," *Mathematics in Computer Science* **4**(4) (2010) 389-429; B. Chow & F. Luo, "Combinatorial Ricci flows on surfaces," *J. Differential Geometry* **63** (2003) 97-129.

[18] J. Peiro & S. Sherwin, *Finite Difference, Finite Element and Finite Volume Methods For Partial Differential Equations,* in Handbook of Materials Modeling, Volume 1, Methods and Models, Springer, 2005.

[19] S. Humphries, Jr., *Finite-Element Methods for Electromagnetism*, *Field Solutions on Computers* (ISBN 0-8493-1668-5) (Taylor and Francis, Boca Raton, 1997).

[20] W. Thurston, *Three-dimensional geometry and topology,* Vol. 1. Edited by Silvio Levy, Princeton Mathematical Series, 35, (Princeton University Press, Princeton, NJ, 1997).

[21] G. Perelman, "The entropy formula for the Ricci flow and its geometric applications," preprint, math.DG/0211159; G. Perelman, "Ricci flow with surgery on three-manifolds," preprint, math.DG/0303109; & G. Perelman, "Finite extinction time for the solutions to the Ricci flow on certain three-manifolds," preprint, *math.DG/0307245*.

[22] M. Hein and M. Maier, "Manifold Denoising," in *Advances in Neural Information Processing Systems* **19** (NIPS 2006). (Eds.) B. Schlkopf, J.C. Platt and T. Hofmann (2007).

[23] P. M. Alsing, H. A. Blair, M. Corne, G. Jones, W. A. Miller, K. Mischaikow & V. Nanda, "Topological Signals of Singularities in Ricci Flow," *Axioms* **6**(3) (2017) 24.

[24] S. Jackson, R. Pourhasan & H. Verlinde, "Geometric RG flow," (2013) *arXiv:1312.6914*.

[25] M. Carfora & S. Romano, "Quantum fluctuations and geometry: from graph counting to Ricci flow," (2009) *arXiv:0902.2061v3 [hep-th]*.

[26] W. A. Miller, J. R. McDonald, P. M. Alsing, D. X. Gu & S-T Yau, "Simplicial Ricci Flow," *Commun. Math. Phys.* **329** 579-608 (2014).

[27] P. M. Alsing, J. R. McDonald & W. A. Miller, "The simplicial Ricci tensor," *Class. Quantum Grav.* **28** (2011) 155007 (17 pp).

[28] J. R. McDonald, W. A. Miller, P. M Alsing, X. D. Gu, X. Wang & S-T Yau, "On exterior calculus and curvature in piecewise-flat manifolds," *paper submitted to J. Math. Phys.* (2012) arxiv.org/abs/1212.0919.

[29] D. Glickenstein, D. Champion and A. Young, "Regge's Einstein-Hilbert functional on the double tetrahedron," *Differential Geom. Appl.* **29** (2011), 109-124, doi:10.1016/jdifgeo.2010.10.001.

[30] D. Glickenstein, "Discrete conformal variations and scalar curvature on piecewise flat two- and three-dimensional manifolds," *J. Diff. Geom.* **87** (2011) 201-238.

[31] D. Glickenstein, "Geometric triangulations and discrete Laplacians on manifolds," *arXiv:math/0508188 [math.MG]*.

[32] H. Ge, "Discrete Quasi-Einstein Metrics and Combinatorial Curvature Flows in 3-Dimension," *arXiv:1301.3398 [math.DG]*.

[33] R. Forman, "Bochner's method for cell complexes and combinatorial Ricci curvature," *Discrete Comput. Geom.* **29** (2003) 323-374.

[34] R.P. Sreejith, K. Mohanraj, J. Jost,2, E Saucan, and A. Samal, "Forman curvature for complex networks," *J. Stat. Mech.* (2016) 063206, *arXiv:1603.00386v1*.

[35] R. Conboye and W. A. Miller, "Piecewise Flat Curvature and Ricci Flow in Three Dimensions," *Asian J. Math.* **6**(6) (2017) 1063-1098.

[36] T. Regge, "General relativity without coordinates," *Il Nuovo Cimento* **19** (1961) 558-571.

[37] J. McDonald and W. A. Miller, "A geometric construction of the Riemann scalar curvature in Regge Calculus," *Class. Quantum Gravity* **25** (2008) 195017.

[38] S. Angenent & D. Knopf, "An example of neckpinching for Ricci flow on S^{n+1}" . *Math. Res. Lett.* **11** (2004) 493-518.

[39] P. M. Alsing, M. Corne, D. X. Gu, S. Lloyd, W. A. Miller, S. Ray and S-T Yau, "Simplicial Ricci flow: an example of a neck pinch singularity in 3D," *Geom. Imaging Computing* **1**(3) (2014) 303-331.

[40] P. M. Alsing, M. Corne, W. A. Miller and S. Ray, "Equivalence of simplicial Ricci flow for 3D neck pinch geometries," *Geom. Imaging Computing* **1**(3) (2014) 333-366.

[41] M. Weber, J. Jost and E. Saucan,"Forman-Ricci flow for change detection in large dynamic data sets," *Axioms* **5**(4) (2016) 26 *arXiv:1604.06634v2*.

[42] M. Weber, J. Jost and E. Saucan, "Characterizing Complex Networks with Forman-Ricci Curvature and Associated Geometric Flows," *arXiv:1607.08654*.

[43] R. P Sreejith, J. Jost, E. Saucan & A. Samal, "Systematic evaluation of a new combinatorial curvature for complex networks," *Chaos, Solitons & Fractals*, **101**:50-67 (2017).

[44] B. Chow and F. Luo, "Combinatorial Ricci Flows on Surfaces," *J. Differential Geom.* **63**, no. 1 (2003) 97-129.

[45] Y. Lin and S-T Yau, "Ricci curvature and eigenvalue estimate on locally finite graphs," *Math. Res. Lett.* **17** (2010) 343-356.

[46] D. Knopf, "Estimating the trace-free Ricci tensor in Ricci flow," *Journal: Proc. Amer. Math. Soc.* **137** (2009), 3099-3103.

[47] R. Conboye & W. A. Miller, "Picewise flat curvature and Ricci flow in three dimensions," *Asian J. Math.* **21**(6) (2017) 1063–1098.

[48] P. M. Alsing, W. A. Miller & S-T Yau, "A realization of Thurston's geometrization: discrete Ricci flow with surgery," *Annals of Mathematical Sciences and Applications* (2018) in press; arXiv: 1709.08494.

[49] W. A. Miller, S. Ray, M-T Wang & S-T Yau, "Wang and Yau's quasi-local energy for an extreme Kerr spacetime," *Class. Quantum Grav.* (2018) in press; CQG-104058.R2, 2018; arXiv: 1708.07532.

[50] R. Forman, "Bochner's method for cell complexes and combinatorial Ricci curvature," *Discrete Comput. Geom.* **29** (2003) 323–374.

[51] R. P. Sreejith, K. Mohanraj, J. Jost, E. Saucan, & A. Samal, "Forman curvature for complex networks," *J. Stat. Mech.* **20** (2016) 063206; arXiv:1603.00386v1.

[52] M. Weber, J. Jost & E. Saucan, "Forman-Ricci flow for change detection in large dynamic data sets,," *Axioms* **5**(4) (2016) 26.

[53] M-T Wang & S-T Yau, "Isometric embeddings into the Minkowski space and the new quasi-local mass," *Commun. Math. Phys.* **288** (2009) 919–942.