

Washington University in St. Louis

## Washington University Open Scholarship

---

Spring 2017

Washington University  
Senior Honors Thesis Abstracts

---

Spring 2017

### Nonabelian Group Based Cryptography

Timothy (Tim) Huber

*Washington University in St. Louis*

Follow this and additional works at: [https://openscholarship.wustl.edu/wushta\\_spr2017](https://openscholarship.wustl.edu/wushta_spr2017)

---

#### Recommended Citation

Huber, Timothy (Tim), "Nonabelian Group Based Cryptography" (2017). *Spring 2017*. 52.  
[https://openscholarship.wustl.edu/wushta\\_spr2017/52](https://openscholarship.wustl.edu/wushta_spr2017/52)

This Abstract for College of Arts & Sciences is brought to you for free and open access by the Washington University

Senior Honors Thesis Abstracts at Washington University Open Scholarship. It has been accepted for inclusion in Spring 2017 by an authorized administrator of Washington University Open Scholarship. For more information, please contact [digital@wumail.wustl.edu](mailto:digital@wumail.wustl.edu).

# NONABELIAN GROUP BASED CRYPTOGRAPHY

*Timothy (Tim) Huber*

*Mentor: John Shareshian*

Concerns over the security of RSA public-key cryptography with the potential development of quantum computers renewed interest in novel cryptosystems that do not rely on commutative groups. We provide an introduction to public-key cryptography along with an explanation of the AAG and Ko-Lee key agreement protocols with their originally proposed platform group, the braid group. We will then discuss two successful attacks against the AAG cryptosystem with consideration for practical concerns and known empirical results.