



Summer 7-29-2014

Simmons' Research Aims to Improve Function for Online Security

Danielle Kamp
Illinois Wesleyan University

Follow this and additional works at: <https://digitalcommons.iwu.edu/news>

Recommended Citation

Kamp, Danielle, "Simmons' Research Aims to Improve Function for Online Security" (2014).
News and Events. 2421.
<https://digitalcommons.iwu.edu/news/2421>

This Article is protected by copyright and/or related rights. It has been brought to you by Digital Commons @ IWU with permission from the rights-holder(s). You are free to use this material in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/ or on the work itself. This material has been accepted for inclusion by faculty at Illinois Wesleyan University. For more information, please contact digitalcommons@iwu.edu.

©Copyright is owned by the author of this document.

Simmons' Research Aims to Improve Function for Online Security

July 29, 2014

BLOOMINGTON, Ill. — Illinois Wesleyan University student Thomas Simmons '15 (Evergreen Park, Ill.) is spending his summer studying ways to improve your security.

It's not physical safety Simmons is concerned with, but how to improve safer computing. As an [Eckley Summer Scholar and Artist](#), Simmons is studying ways to improve a mathematical function that can be used to perform cryptography as it relates to computerized encoding of secret messages for security purposes.

"Cryptography is all around us, and if implemented well we do not even notice it," said Simmons, a [computer science](#) major. "Every time we secure our communications, use online banking, check our email or buy something from Amazon we are using cryptography."



Tom Simmons '15

Simmons said he became enamored with cryptography during his first year at Illinois Wesleyan. After consulting with Assistant Professor of [Mathematics](#) Andrew Shallue, his faculty mentor for the Eckley project and an expert on algorithmic number theory and its applications to cryptography, Simmons decided to base his research on a function created by French researcher Thomas Icart that maps numbers to points on a curve.

"This function is used in cryptography to translate a numerical message onto the curve, where it is then scrambled," said Shallue. "The goal is to improve the coverage of the Icart function, so that the image includes a larger proportion of the total number of points."

More coverage will result in improved computer security in terms of protection against hackers because there are more password possibilities for the attacker to check.

So far, Simmons and Shallue have been able to increase coverage through discovering patterns in the Icart function, but at the risk of increasing the computation time. They believe with further research and a better understanding of Icart's function, additional improvements can be made.

"I am extremely excited to be an Eckley Scholar," Simmons said. "Having the opportunity to dedicate my summer to research a topic I enjoy is an enormous reward, but the Eckley Scholar distinction is also an honor to carry."

The Eckley Summer Scholars and Artists endowment supports summer research and creative activity for several students each year, enabling them to stay on campus over the summer under the direction of faculty mentors. The program was established as one aspect of a major gift to the University by President Emeritus Robert S. Eckley, his wife Nell and the Eckley Family Foundation, shortly before he passed away in 2012.

[See all 2014 Eckley Scholars](#)

Contact: Danielle Kamp '15, (309) 556-3181, univcomm@iwu.edu