**Store, Forget, and Check: Using algebraic signatures to check remotely administered storage**

Fr. Thomas Schwarz, S. J.

1:00 p.m., Monday, April 11, 2016

**Abstract**

The emerging use of the Internet for remote storage and backup has led to the problem of verifying that storage sites in a distributed system indeed store the data; this must often be done in the absence of knowledge of what the data should be. We use m/n erasure-correcting coding to safeguard the stored data and use algebraic signatures—hash functions with algebraic properties—for verification. Our scheme primarily utilizes one such algebraic property: taking a signature of parity gives the same result as taking the parity of the signatures. To make our scheme collusion-resistant, we blind data and parity by XORing them with a pseudo-random stream. Our scheme has three advantages over existing techniques. First, it uses only small messages for verification, an attractive property in a P2P setting where the storing peers often only have a small upstream pipe. Second, it allows verification of challenges across random data without the need for the challenger to compare against the original data. Third, it is highly resistant to coordinated attempts to undetectably modify data. These signature techniques are very fast, running at tens to hundreds of megabytes per second. Because of these properties, the use of algebraic signatures will permit the construction of large-scale distributed storage systems in which large amounts of storage can be verified with minimal network bandwidth.

Thomas Schwarz SJ is a California Jesuit with a doctorate in Mathematics (Hagen, Germany) and a Ph. D. in Computer Science from the University of California at San Diego. His research interests are in security and systems reliability, especially storage systems. He is author of more than 100 publications and an Adjunct Professor at the University of California at Santa Cruz and the University of Houston. The last five years, he taught in Latin America at the Universidad Católica del Uruguay and Universidad Centroamericana in El Salvador.

1313 W. Wisconsin Avenue, Cudahy Hall, Room 401, Milwaukee, WI 53201-1881

For further information:  [http://www.mscs.mu.edu/mscs/resources/colloquium.html](http://www.mscs.mu.edu/mscs/resources/colloquium.html), or contact Dr. Naveen Bansal: 414-288-5290, naveen.bansal@marquette.edu.

**PRE-COLLOQUIUM REFRESHMENTS SERVED IN ROOM 342 AT 12:30 P.M.**