Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption
AzTE Case # M12-210P

Background
Encryption schemes are used to protect information transmitted between computers. This includes information used by the military, banking, and emails transmitted through the Internet. As computers have become more advanced, better encryption techniques are needed to keep information secure. Ciphertext Policy Attribute Encryption (CP-ABE) enforces expressive data access policies and each policy consists of a number of attributes. Most existing CP-ABE schemes incur very large ciphertext file size that increases linearly with respect to the number of attributes in the access policy. These schemes are bulky and can become very large files.

Invention Description
Researchers at Arizona State University have developed a Constant Size Ciphertext Policy Attribute Encryption program. Encryption with this method significantly reduces the ciphertext to a constant size with any given number of attributes. The program includes a hidden policy construction that protects the recipient’s privacy. This program is more flexible than existing programs. Additionally, the program reduces the storage size and the time required to communicate information.

Potential Applications
- Military
- Business and Industry
- Communication

Benefits and Advantages
- **Lower Costs** – Program uses less computer storage
- **More Secure** – Better security of information
- **Retrofit** – Adaptable to existing computers