

Secure Content Validation: Performance

John Horst

27 April 2007



Problem Statement

- Information is Everywhere.
- Is information valid?
- Source revocation?
- In a confidential environment?

Intelligence Reports/News Articles

- Document
 - Information
 - Confidential Sources
- Producer wants protect sources and methods
- End users need information
- Derived information
- Revocation?
- Solution: Secure Content Validation

Secure Content Validation Models

- Trust Third Party (TTP)
 - Public Key Cryptography
- Public Key Encryption (PKE, PKE*)
 - Homomorphic Encryption
 - RSA, El Gamal, Paillier...
 - Threshold Encryption
 - Paillier

Implementation

- C
 - Paillier (TTP)
 - Paillier Threshold Encryption (PKE,PKE*)
 - Translated from Java implementation
- GMP
 - **GNU Multiple Precision Arithmetic Library**

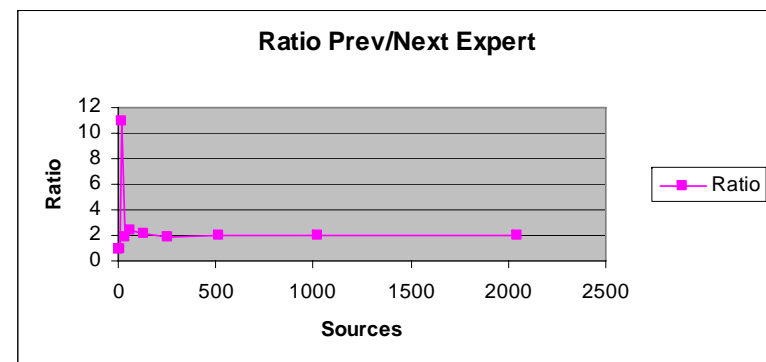
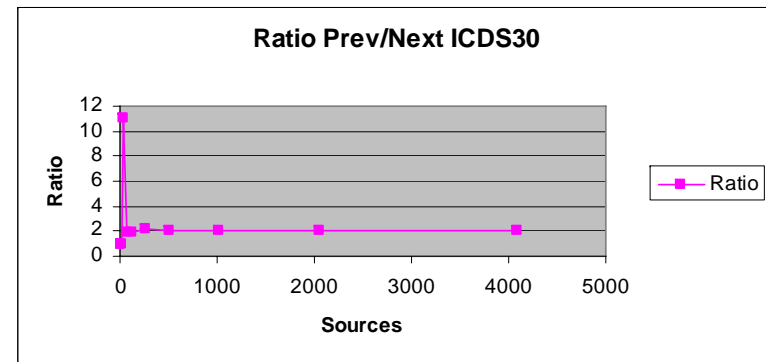
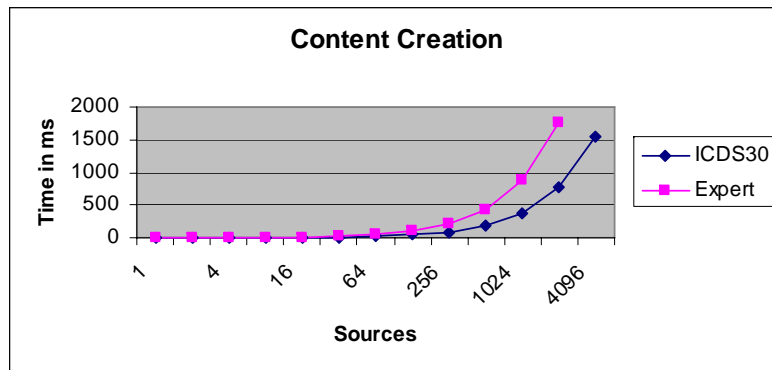
What Constitutes Performance

- Communication
 - Source Revocation
 - Content Validation
 - Common Source Detection
- Calculation
 - Content Creation
 - Content Validation
 - Common Source Detection
- Calculation > Communication

Theoretical – TTP Model

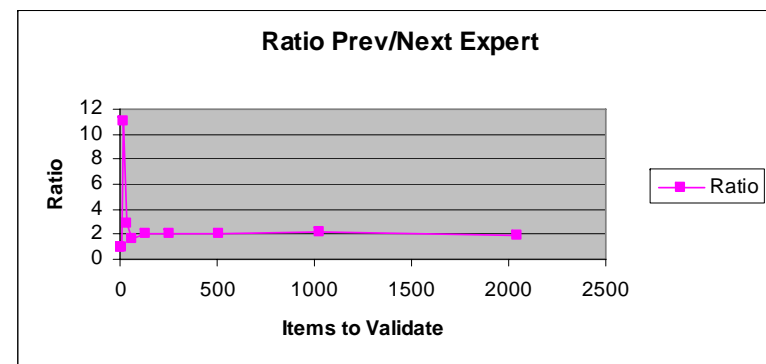
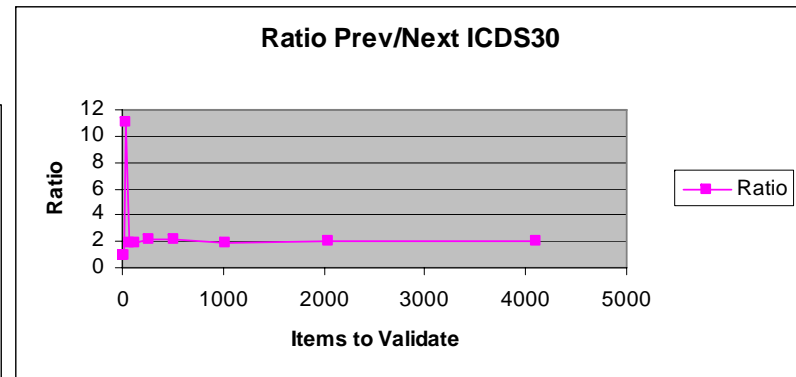
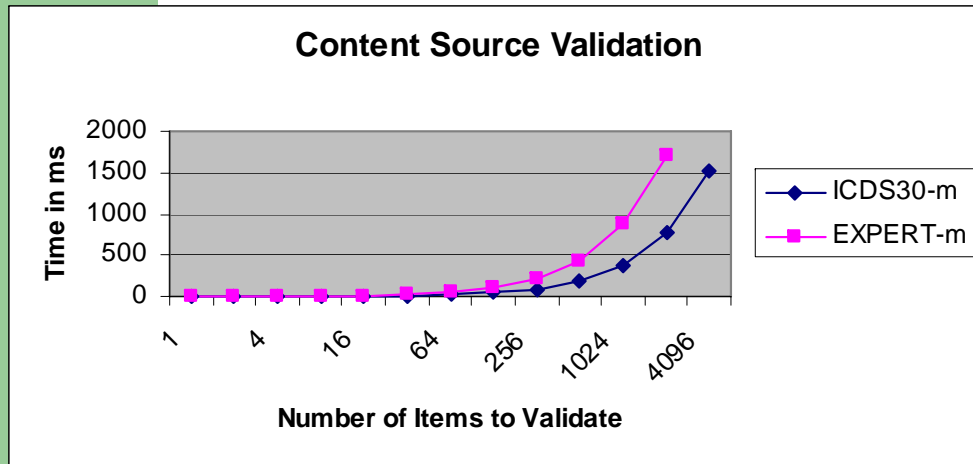
- Content Creation
 - $O(n)$
- Content Validation
 - $O(|V|)$
- Common Source Detection
 - $O(m * N_m)$

TTP-Content Creation Performance



TTP-Common Source Detection

TTP-Content Validation Performance



Theoretical – PKE Model

- Content Creation
 - $O(n)$
- Content Validation
 - $O(|RL| * |V|)$
- Common Source Detection
 - $O(m * N_1 * N_m)$

Sources

- Based on Secure Content Validation
 - Mummorthy Murugesan
 - Wei Jiang
- P. Paillier, .Public key cryptosystems based on composite degree residuosity classes,. in *Advances in Cryptology - Eurocrypt '99 Proceedings, LNCS 1592*. Springer-Verlag, 1999, pp. 223.238.