Temasek Defence Systems Institute

Temasek Defence Systems Institute

Secret Sharing Schemes and Advanced Encryption Standard

MAJ Lim Bing Yong, RSAF
Dr. Pante Stanica (Thesis Advisor)
Dr. David Canright (Second Reader)

Content:

- Identify a simplified methodology to reconstruct a secret that is distributed using Shamir's Secret Sharing Scheme

- Main Research Ideas
  - Dealer hides a secret using Shamir's Secret Sharing Scheme (using {k,n} threshold scheme)
  - Using pre-existing mathematical conjectures (Pillai's conjecture and Fermat-Catalan conjecture) to simplify a monic polynomial so as to improve the efficiency in recovering the secret
  - Simplifying a k-degree polynomial

$$[f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_k x^k] \rightarrow [f(x) = (x+\alpha)^k - b_0]$$

- Research Results
  - From $[f(x) = (x+\alpha)^k - b_0]$, one just needs to find α and b_0, from the 2 public shares that are readily available [public shares provide value of f(x) and x]
  - Instead of the standard k shares to reconstruct the secret in {k,n} scheme, this method requires only 2 shares to perform an educated guess
  - The more shares gathered, the easier it is to implement educated guess

- Potential applications of the research
  - Uncovers a potential weakness in current secret sharing schemes
  - Applicable to Advanced Encryption Standard, where RNGs are often used in algorithms
  - Research found a potential weakness in cracking coefficients of polynomials generated by RNGs

- Follow-up research activities
  - Using quadratic polynomials for simplification instead of linear polynomials

    For e.g., $[f(x) = (x+\alpha)^m (x+\beta)^n - b_0]$, where (m+n) = degree of original polynomial
  - Potentially applicable to non-monic polynomials

NUS National University of Singapore