# DETEKSI DAN IDENTIFIKASI KECURANGAN PADA SKEMA PEMBAGIAN RAHASIA SHAMIR MENGGUNAKAN VERIFIKASI BERBASIS PARITAS

**MIRZA FARHAN AZHARI**

**PROGRAM STUDI MATEMATIKA TERAPAN**
**SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA**
**INSTITUT PERTANIAN BOGOR**
**BOGOR**
**2026**

# PERNYATAAN MENGENAI TESIS DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tesis dengan judul "Deteksi dan Identifikasi Kecurangan pada Skema Pembagian Rahasia Shamir Menggunakan Verifikasi Berbasis Paritas" adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan oleh penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir tesis ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Agustus 2026

Mirza Farhan Azhari
M0502241005

# RINGKASAN

MIRZA FARHAN AZHARI. Deteksi dan Identifikasi Kecurangan pada Skema Pembagian Rahasia Shamir Menggunakan Verifikasi Berbasis Paritas. Dibimbing oleh SUGI GURITMAN dan JAHARUDDIN.

Pengelolaan kunci kriptografi merupakan aspek penting dalam sistem keamanan modern karena berkaitan dengan kerahasiaan, integritas, dan ketersediaan informasi. Skema pembagian rahasia Shamir memungkinkan suatu rahasia dibagi menjadi beberapa keping dan hanya dapat dipulihkan apabila sejumlah minimum keping digabungkan. Namun, skema Shamir standar mengasumsikan bahwa setiap partisipan menyerahkan keping yang valid, sehingga keping yang dimodifikasi akibat kesalahan atau kecurangan dapat menghasilkan rahasia yang salah tidak dapat terdeteksi.

Penelitian ini bertujuan menguraikan peran parameter verifikasi berbasis paritas dalam skema ambang batas Shamir termodifikasi, termasuk proses pembangkitan dan pengikatannya terhadap setiap keping rahasia pada tahap distribusi. Penelitian ini juga menganalisis mekanisme verifikasi paritas di bawah *authenticated parity model* dalam mendeteksi dan mengidentifikasi keping rahasia yang rusak selama rekonstruksi, serta menentukan kondisi yang diperlukan untuk koreksi dan pemulihan rahasia asli. Selain itu, penelitian ini mengevaluasi beban komputasi tambahan dari rekonstruksi rekursif yang diusulkan dibandingkan metode yang telah ada, serta *trade-off* antara efisiensi penyimpanan keping rahasia dan kinerja rekonstruksi berdasarkan batas bawah OKS.

Penelitian dilakukan melalui pendekatan konstruktif-teoretis yang disertai simulasi numerik, diawali dengan kajian literatur mengenai skema pembagian rahasia Shamir dan mekanisme deteksi kecurangan di bawah kerangka Ogata–Kurosawa–Stinson (OKS). Skema bekerja pada lapangan hingga dengan bilangan prima sebagai modulus; *dealer* membangkitkan polinomial rahasia berderajat $k-1$, dan setiap partisipan memperoleh keping rahasia beserta parameter cek paritas, sehingga setiap keping direpresentasikan sebagai tripel identitas partisipan, nilai keping, dan parameter paritas yang diasumsikan tersimpan secara autentik (*authenticated parity model*). Pada tahap rekonstruksi, *combiner* memverifikasi setiap keping melalui relasi paritas, mengidentifikasi dan mengoreksi keping yang tidak sesuai, sebelum rahasia dipulihkan melalui formulasi rekursif berbasis struktur matriks Vandermonde tanpa menghitung invers matriks secara penuh.

Hasil penelitian menunjukkan bahwa mekanisme paritas mampu mendeteksi, mengidentifikasi, dan mengoreksi keping tidak valid tanpa memerlukan pemeriksaan kombinatorik terhadap seluruh sub himpunan partisipan, serta tetap mempertahankan sifat kerahasiaan sempurna dari skema Shamir. Penambahan mekanisme verifikasi tidak menyebabkan peningkatan orde komputasi yang besar, meskipun laju informasi efektif menurun akibat tambahan parameter paritas pada setiap keping. Simulasi empiris menunjukkan bahwa waktu eksekusi tetap berada pada skala milidetik dan skema tetap fleksibel terhadap perubahan urutan penggabungan keping serta penambahan peserta baru.

Penelitian ini menyimpulkan bahwa skema Shamir termodifikasi dengan parameter verifikasi berbasis paritas, yang direpresentasikan sebagai tripel identitas partisipan, nilai keping, dan parameter paritas, mampu mendeteksi,

mengidentifikasi, dan mengoreksi keping rahasia yang dimodifikasi pada tahap rekonstruksi di bawah *authenticated parity model*, sekaligus tetap mempertahankan sifat kerahasiaan sempurna dari skema Shamir. Penambahan parameter paritas menurunkan laju informasi efektif menjadi $\rho = 1/2$, namun rekonstruksi rekursif berbasis metode selisih terbagi Newton tetap efisien tanpa menghitung invers matriks Vandermonde secara penuh, sehingga penambahan mekanisme verifikasi tidak menyebabkan lonjakan kompleksitas komputasi. Simulasi empiris menunjukkan bahwa waktu eksekusi tetap berada pada skala praktis, sehingga skema yang diusulkan dapat dipandang sebagai perluasan skema Shamir yang menyediakan kemampuan verifikasi dan koreksi dengan *overhead* terkendali sekaligus menjadi dasar matematis bagi pengembangan skema pembagian rahasia yang lebih adaptif terhadap manipulasi keping.

Kata kunci: cek paritas, formulasi rekursif, kecurangan, pembagian rahasia Shamir.

# SUMMARY

MIRZA FARHAN AZHARI. Cheating Detection and Identification in Shamir Secret Sharing Scheme Using Parity-Based Verification. Supervised by SUGI GURITMAN and JAHARUDDIN.

Cryptographic key management is an essential aspect of modern security systems because it is directly related to the confidentiality, integrity, and availability of information. Shamir's secret sharing scheme allows a secret to be divided into several shares and recovered only when a minimum number of shares are combined. However, the standard Shamir scheme assumes that every participant submits a valid share, thus, a share modified due to error or cheating can cause the reconstruction to produce an incorrect secret without being detected.

This study aims to describe the role of the parity-based verification parameter in the modified Shamir threshold scheme, including its generation and binding to each share during the distribution phase. This study also analyses the parity-based verification mechanism under the authenticated parity model in detecting and identifying corrupted shares during reconstruction, as well as determining the conditions required for correction and recovery of the original secret. In addition, this study evaluates the additional computational overhead of the proposed recursive reconstruction compared with existing methods, as well as the trade-off between share storage efficiency and reconstruction performance based on the OKS lower bound.

The study was conducted using a constructive-theoretical approach supported by numerical simulations, beginning with a literature review on Shamir's secret sharing scheme and cheating-detection mechanisms under the Ogata–Kurosawa–Stinson (OKS) framework. The scheme operates over a finite field with a prime modulus; the dealer generates a secret polynomial of degree $k-1$, and each participant obtains a share together with a parity-check parameter, so that each share is represented as a triplet of the participant's identity, share value, and parity parameter, assumed to be stored authentically under the authenticated parity model. During reconstruction, the combiner verifies each share through the parity relation, identifies and corrects inconsistent shares before the secret is recovered using a recursive formulation based on the Vandermonde matrix structure without computing the full matrix inverse. Numerical simulations were carried out using Python and Maple to verify the scheme's construction and to analyze its security, performance, and computational complexity.

The results show that the proposed parity mechanism is able to detect, identify, and correct invalid shares without requiring combinatorial checking over all participant subsets, while still preserving the perfect secrecy property of Shamir's scheme. The addition of the verification mechanism does not cause a significant increase in computational complexity, although the effective information rate decreases due to the additional parity parameter carried by each share. Empirical simulations show that execution time remains on the millisecond scale and that the scheme remains flexible with respect to changes in the order of share combination and the addition of new participants.

This study concludes that the modified Shamir scheme with parity-based verification, represented as a triplet of participant identity, share value, and parity

parameter, is able to detect, identify, and correct modified shares during reconstruction under the authenticated parity model, while still preserving the perfect secrecy property of Shamir's scheme. The addition of the parity parameter reduces the effective information rate to $\rho = 1/2$, yet the recursive reconstruction based on Newton's divided-difference method remains efficient without computing the full inverse of the Vandermonde matrix, preventing the added verification mechanism from causing a significant increase in computational complexity. Empirical simulations show that execution time remains within a practical scale, allowing the proposed scheme can be regarded as an extension of Shamir's scheme that provides verification and correction capability with controlled overhead, while also serving as a mathematical basis for developing secret sharing schemes that are more adaptive to share manipulation.

*Keywords*: cheating, parity check, recursive formulation, Shamir secret sharing.

# DETEKSI DAN IDENTIFIKASI KECURANGAN PADA SKEMA PEMBAGIAN RAHASIA SHAMIR MENGGUNAKAN VERIFIKASI BERBASIS PARITAS

**MIRZA FARHAN AZHARI**

Tesis
sebagai salah satu syarat untuk memperoleh gelar
Magister Matematika pada
Program Studi Matematika Terapan

**PROGRAM STUDI MATEMATIKA TERAPAN**
**SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA**
**INSTITUT PERTANIAN BOGOR**
**BOGOR**
**2026**

Tim Penguji pada Ujian Tesis:
1 Prof. Dr. Ir. Sri Nurdiati, M.Sc.

Judul Tesis : Deteksi dan Identifikasi Kecurangan pada Skema Pembagian Rahasia Shamir Menggunakan Verifikasi Berbasis Paritas

Nama : Mirza Farhan Azhari
NIM : M0502241005

Disetujui oleh

Pembimbing 1:
Dr. Drs. Sugi Guritman

Pembimbing 2:
Prof. Dr. Drs. Jaharuddin, M.S.

Diketahui oleh

Ketua Program Studi:
Prof. Dr. Drs. Jaharuddin, M.S.
NIP. 196511021993021001

Dekan Sekolah Sains Data, Matematika, dan Informatika:
Prof. Dr. Ir. Agus Buono, M.Si., M.Kom.
NIP. 196607021993011001

Tanggal Ujian: 13 Agustus 2026 Tanggal Lulus:

# PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanahu wa ta'ala atas segala karunia-Nya sehingga tesis ini dapat diselesaikan. Penelitian ini dilaksanakan pada Januari–Februari 2026 dengan judul "Deteksi dan Identifikasi Kecurangan pada Skema Pembagian Rahasia Shamir Menggunakan Verifikasi Berbasis Paritas". Penyelesaian tesis ini tidak terlepas dari bantuan, arahan, dan dukungan berbagai pihak.

Terima kasih penulis ucapkan kepada

1. Dr. Drs. Sugi Guritman selaku pembimbing utama dan Prof. Dr. Drs. Jaharuddin, M.S. selaku pembimbing kedua yang telah memberikan arahan, bimbingan, serta saran konstruktif selama proses penyusunan karya ilmiah ini.
2. Kedua orang tua penulis, Cari Azhari dan Ernita Lisnovia, atas segala dukungan moral, spiritual, dan finansial yang tidak pernah terputus. Doa dan pengorbanan beliau menjadi sumber kekuatan utama dalam menyelesaikan studi ini.
3. Rekan-rekan dan berbagai pihak yang telah membantu dalam menyediakan akses terhadap literatur ilmiah yang diperlukan selama proses penelitian dan penulisan tesis ini.
4. Seluruh penulis dan peneliti yang karya-karyanya dirujuk dalam tesis ini, yang telah memberikan landasan ilmiah dan memperkaya diskursus akademik dalam penelitian ini.
5. Teman-teman Bogorian yang senantiasa menjadi ruang jeda dari kejenuhan akademik serta pengingat bahwa kehidupan tidak hanya tentang tenggat waktu.
6. Rekan-rekan mahasiswa S2 MAT yang selalu berbagi informasi terkait administrasi maupun dinamika non-akademik selama masa studi.
7. Seluruh staf Departemen Matematika IPB atas bantuan dan pelayanan akademik selama penulis menempuh pendidikan.
8. Sahabat baik penulis, Gibran dan Sidik, yang dengan caranya sendiri selalu hadir untuk memastikan penulis tidak benar-benar tersesat di tengah proses yang panjang ini.

Semoga karya ilmiah ini memberi dampak nyata bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Agustus 2026

*Mirza Farhan Azhari*

# DAFTAR ISI

# DAFTAR TABEL



# DAFTAR GAMBAR



# DAFTAR LAMPIRAN