Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based* *Single-board Computer*

Oleh:

Renci Kiel Palembangan

NIM: 672017151

Program Studi Teknik Informatika

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Januari 2024

Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based* *Single-board Computer*

Artikel Ilmiah

Diajukan Kepada

Fakultas Teknologi Informasi

Untuk Memperoleh Gelar Sarjana Komputer

Oleh:

Renci Kiel Palembangan

NIM: 672017151

Program Studi Teknik Informatika

Fakultas Teknologi Informasi

Univesitas Kristen Satya Wacana

Januari 2024

Lembar Pengesahan

Judul Artikel	: Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based Single-board Computer*
Nama Mahasiswa	: Renci Kiel Palembangan
NIM	: 672017151
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Theophilus Wellem, S.T., M.S., Ph.D.
Pembimbing

Mengesahkan,

Prof. Ir. Daniel H. F. Manongga, M.Sc., Ph.D.	Budhi Kristianto, S.Kom., M.Sc., Ph.D.
Dekan	Ketua Program Studi

Dinyatakan Lulus Proses Review Tanggal : 13 Februari 2024

Reviewer :

- Dr. Wiwin Sulistyo, S.T., M.Kom.

Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based Single-board Computer*

Oleh,

Renci Kiel Palembangan
672017151

LAPORAN PENELITIAN

Diajukan Kepada Program Studi Teknik Informatika guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Theophilus Wellem, S.T., M.S., Ph.D.
Pembimbing

Diketahui oleh,

Prof. Ir. Daniel H. F. Manongga, M.Sc., Ph.D.
Dekan

Budhi Kristianto, S.Kom., M.Sc., Ph.D.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2024

Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based Single-board Computer*

Oleh,

Renci Kiel Palembangan
672017151

ARTIKEL ILMIAH

Diajukan Kepada Program Studi Teknik Informatika guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Theophilus Wellem, S.T., M.S., Ph.D.
Pembimbing

Diketahui oleh,

Prof. Ir. Daniel H. F. Manongga, M.Sc., Ph.D.
Dekan

Budhi Kristianto, S.Kom., M.Sc., Ph.D.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2024

Pernyataan

Yang bertandatangan di bawah ini,

Nama Mahasiswa	: Renci Kiel Palembangan
NIM	: 672017151
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul:

Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based* *Single-board Computer*

yang dibimbing oleh:

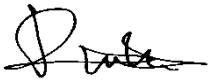
Theophilus Wellem S.T., M.S., Ph.D.

adalah benar-benar hasil karya saya.

Pada tugas akhir ini tidak terdapat keseluruhan atau sebagian tulisan atau gagasan orang lain yang saya ambil dengan cara menyalin atau meniru dalam bentuk rangkaian kalimat atau gambar serta simbol yang saya aku seolah-olah sebagai karya saya tanpa memberikan pengakuan pada penulis atau sumber aslinya.

Salatiga, 31 Januari 2024

Yang memberi pernyataan



Renci Kiel Palembangan

Evaluasi Kinerja Algoritma CRYSTALS-Kyber pada ARM-*based Single-board Computer*

Renci Kiel Palembangan[1], **Theophilus Wellem**[*2]

[1,2)]Program Studi Teknik Informatika, Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo no. 1-10 Blotongan, Salatiga, Jawa Tengah, 50715
Email: 672017151@student.uksw.edu[1], theophilus.wellem@uksw.edu[*2]

Abstrak **–** *CRYSTALS-Kyber merupakan algoritma key-encapsulation mechanism (KEM) yang terpilih pada putaran ketiga proses standardisasi post-quantum cryptography (PQC). Penelitian ini melakukan evaluasi algoritma Kyber-512 dan Kyber-512-90s dalam lingkungan container pada single-board computer berbasis prosesor ARM. Evaluasi dilakukan dengan membandingkan implementasi symmetric primitives yang digunakan Kyber dengan reference implementation (liboqs), OpenSSL, dan crypto extension. Hasil evaluasi menunjukkan bahwa implementasi dengan OpenSSL dapat meningkatkan kinerja (waktu eksekusi dalam CPU cycle) hingga 1.71–2.01× pada Cortex-A7 dibandingkan dengan reference implementation. Untuk Kyber512-90s pada Cortex-A53, implementasi dengan OpenSSL dan crypto extension menunjukkan peningkatan kinerja berkisar antara 1.36–1.69×.*

Kata Kunci **–** Kyber512; *post-quantum cryptography*; *container*; ARM

Abstract **–** *CRYSTALS-Kyber is a key-encapsulation mechanism (KEM) algorithm selected in the third round of the post-quantum cryptography (PQC) standardization process. This research evaluates the Kyber-512 and Kyber-512-90s algorithms in a container environment on a single-board computer based on an ARM processor. Evaluation was carried out by comparing the implementation of symmetric primitives used by Kyber with the reference implementation (liboqs), OpenSSL, and crypto extensions. Evaluation results show that implementation with OpenSSL can increase performance (execution time in CPU cycles) by up to 1.71–2.01× on Cortex-A7 compared to the reference implementation. For Kyber512-90s on Cortex-A53, implementations with OpenSSL and crypto extensions show performance gains ranging from 1.36–1.69×.*

Keywords **–** Kyber512; *post-quantum cryptography*; *container*; ARM