# OriSign: Spesifikasi Formal Algoritma SQISIGN Round 2 dengan Contoh dan Analogi

**Daftar Isi**

## Status

Dokumen ini adalah spesifikasi formal SQISIGN Round 2, dilengkapi dengan contoh dan analogi matematika untuk membantu pemahaman.

**(Analogi)**: Bayangkan algoritma ini seperti sistem **brankas digital**: kunci rahasia adalah kombinasi rahasia, kunci publik adalah brankas yang terlihat semua orang, dan tanda tangan adalah bukti bahwa Anda bisa membuka brankas tanpa membocorkan kombinasi.

# 1 Tujuan dan Model Keamanan

SQISIGN Round 2 adalah skema tanda tangan pasca-kuantum berbasis kurva eliptik supersingular dan aljabar kuaternion.

Keamanan bergantung pada:

- Masalah pencarian jalur isogeni supersingular.
- Masalah persamaan norma ideal kuaternion.
- Rekonstruksi isogeni dari data kernel/interpolasi.

**(Analogi)**: Seperti mencoba menemukan jalan rahasia melalui labirin yang ukurannya **eksponensial**, dengan pintu yang hanya bisa dibuka dengan kombinasi rahasia.

# 2 Parameter Sistem

$$p = \beta \cdot 2^{\alpha} - 1, \quad p \equiv 3 \pmod 4.$$

**(Contoh)**: Jika $\alpha = 100$ dan $\beta = 3$, maka $p = 3 \cdot 2^{100} - 1$ adalah bilangan prima besar.

## 2.1 Parameter Utama

- $e_{\text{sk}}$: Panjang ideal rahasia. **(Contoh / Analogi)**: Seperti jumlah putaran kombinasi brankas; $2^{e_{\text{sk}}} \approx \sqrt{p}$ berarti ada **triliunan kemungkinan**.
- $D_{\text{mix}}$: Derajat komitmen, bilangan prima lebih besar dari $2^{4\lambda}$. **(Analogi)**: Brankas palsu yang bisa diverifikasi tapi tidak mempermudah penyerang.
- $e_{\text{chl}}$: Panjang isogeni tantangan. **(Analogi)**: Panjang pertanyaan dari auditor untuk menguji brankas.
- $D_{\text{rsp}}$: Derajat respons, $2^{e_{\text{rsp}}}$. **(Contoh / Analogi)**: Bukti bahwa Anda bisa membuka pintu tertentu tanpa menunjukkan seluruh kombinasi.

## 2.2 Fungsi Hash

$$H : \{0,1\}^* \to \{0,1\}^{e_{\text{chl}}}, \quad \text{dengan SHAKE-256}$$

**(Analogi)**: Menghasilkan pertanyaan auditor dari pesan dan kunci publik secara deterministik.

# 3 Aritmetika Lapangan Hingga

**(Contoh nyata)**: Jika $p = 7$, maka $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, dengan operasi modulo $p$:

$$3 + 5 \equiv 1 \pmod 7, \quad 2 \cdot 4 \equiv 1 \pmod 7.$$

## 3.1 Ekstensi Kuadrat $\mathbb{F}_{p^2}$

Ambil $i$ sehingga $i^2 = -1 \in \mathbb{F}_p$.

$$x = a + bi, \quad a, b \in \mathbb{F}_p$$

**(Contoh nyata)**: Jika $p = 7$, maka $i^2 \equiv -1 \equiv 6 \pmod 7$, dan

$$x = 2 + 3i \in \mathbb{F}_{7^2}.$$

Operasi dasar:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$
$$(a + bi)^{-1} = \frac{a - bi}{a^2 + b^2} \pmod p$$

**(Contoh)**:

$$x \cdot x^{-1} = (2 + 3i) \cdot (2 - 3i)/(2^2 + 3^2) \equiv 1 \pmod 7$$

# 4 Kurva Eliptik Supersingular

$$E : y^2 = x^3 + Ax + B$$

**(Contoh)**: $E : y^2 = x^3 + 2x + 3$ di $\mathbb{F}_7$ memiliki titik $(0, 2), (1, 3), (2, 1), \ldots$
**(Analogi)**: Papan catur 2D dengan titik-titik yang sah.

# 5 Isogeni Dimensi 2 (Permukaan Abelian)

**(Analogi)**: Dua papan catur identik; isogeni dimensi 2 memindahkan konfigurasi titik dari satu papan ke papan lain.

## 5.1 Definisi

$$\phi : E_1 \times E_1 \to E_2 \times E_2$$

**(Contoh)**: Kernel = $\{(0, 0), (1, 2)\}$, interpolation data digunakan untuk menentukan $\phi$.

# 6 Pengkodean Objek

## 6.1 Kunci Publik dan Rahasia

- Kunci publik $pk = E_{pk}$ (uniform) $\to$ brankas terlihat.
- Kunci rahasia $sk = I_{sk} \to$ kombinasi rahasia.
- Tanda tangan $\sigma = (E_{com}, \text{interpolation data}) \to$ peta titik-titik untuk membuka brankas sementara.

# 7 Algoritma Inti

## 7.1 Pembangkitan Kunci

Ambil ideal acak $I \subset \mathcal{O}_0$, hitung $E_{pk} = E_0/I$. **(Analogi)**: Membuat brankas baru dari kombinasi rahasia.

## 7.2 Penandatanganan

1. Komitmen $E_{com} = E_{pk}/J$, $J$ acak $\rightarrow$ brankas sementara.
2. Tantangan $c \rightarrow$ pilih titik basis $\rightarrow$ interpolasi isogeni.
3. Respons $\rightarrow$ bangun interpolation data $\rightarrow$ bukti mengetahui kombinasi rahasia.

## 7.3 Verifikasi

- Verifikator membangun kembali isogeni $(D, D)$ dari interpolation data.
- Terima jika kernel menghasilkan kodomain $= E_{chl}$.
- **(Analogi)**: Auditor membuka brankas sementara menggunakan peta titik-titik.

# 8 Diagram Alur Penandatanganan

$$\begin{array}{ccc} E_{pk} \times E_{pk} & \xrightarrow{\phi_J} & E_{com} \times E_{com} \\ \Big\downarrow{\scriptstyle \phi_c} & & \Big\downarrow{\scriptstyle \text{interp}} \\ E_{chl} \times E_{chl} & & E_{chl} \times E_{chl} \end{array}$$

# 9 Intuisi Keamanan

Memalsukan tanda tangan berarti membuat interpolation data tanpa mengetahui $I_{sk}$. **(Analogi)**: Seperti mencoba membuka brankas tanpa kombinasi rahasia; labirin kombinasi triliunan kemungkinan.

# 10 Persyaratan Keamanan Implementasi

- Operasi rahasia harus constant-time, tanpa percabangan tergantung nilai rahasia.
- Buffer tetap, randomisasi koordinat, masking, blinding ideal.

# 11 Ringkasan Implementasi

- Kunci rahasia: ideal kiri bernorma $2^{e_{\text{sk}}} \approx \sqrt{p}$.
- Kunci publik: kurva supersingular, uniform.
- Tanda tangan: kurva komitmen + interpolation data.

- Verifikasi: membangun kembali isogeni $(D, D)$ dari interpolation data.
- Tidak ada pertukaran kunci.