

STELLINGEN

accompanying the thesis

ISOGENIES & ISOMETRIES

by

KRIJN CORNELIUS JOHANNES MARIA REIJNDERS

-
1. Probing using the Tate pairing is a magical technique: we learn something about fibers $\varphi^{-1}(P)$ even if we cannot compute φ or $\hat{\varphi}$.
 2. Signatures of schemes based on generalized 1-bit Sigma protocols are too large: isometry-based cryptography must be more bold.
 3. Never start with $\ell = \text{char}(\mathbb{F}_q)$ or $\ell = 2$.
 4. The worst constant-time algorithms are variable time.
 5. In practice, almost every square matrix $\mathbf{A} \in \mathbb{F}_q^{n \times n}$ is invertible.
 6. A line length over 80 characters should *strongly* be avoided.
 7. Whenever someone writes “Clearly,” in a piece of text, replace it by “I think” to improve whatever follows.
 8. Clearly, the Tate pairing is more intuitive than the Weil pairing.
 9. Curves of genus 2 are twice as fun as curves of genus 1.
 10. The α -coefficient is superior to the Montgomery A -coefficient.
-

