**MATTHEW MUSSON**, University of Calgary

*A Second Look at the GHS Attack on the Elliptic Curve Discrete Log Problem*

We take a second look at the GHS Attack on the ECDLP. This time we relax the conditions of Hess' theorem in its analysis and find more curves appearing in the Weil Restriction. Relaxing the conditions of Hess' theorem benefits us especially in the case where curves are defined over $\mathbb{F}_{2^n}$ where $n = 2p, 3p$ or $4p$ for some prime $p$ such that $2^n > 2^{160}$. In particular, we classify all curves appearing via the GHS attack over $\mathbb{F}_{q^2}$ and determine the full security impact on the fields $\mathbb{F}_{q^3}$ and $\mathbb{F}_{q^4}$. Our analysis suggests that the fields $\mathbb{F}_{q^4}$ are bad for elliptic curve cryptography - the first such fields - and should never be used in cryptographic protocols. We then turn our attention to fields of the form $\mathbb{F}_{q^5}$ and discuss the security impact of our findings, focusing on the curves found in the Oakley Key Determination Protocol. Lastly, we discuss ongoing research and open problems concerning this attack.