1147-94-100 **Joseph H Silverman***, Mathematics Department, Box 1917, Brown University, Providence, RI 02912. *The Hidden Quadratic Form Problem.* Preliminary report.

A quadratic form $Q : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is *small* if its coefficients are small, for exmaple chosen from $\{-1, 0, 1\}$. If Q is a small quadratic form and $L \in \mathrm{GL}_n(\mathbb{F}_q)$ is a random invertible linear transformation, then $Q_L := Q \circ L$ is a random-looking quadratic form hiding the small form Q. I will discuss the problem of recovering Q from Q_L and how the difficulty of this problem might be used for various public key protocals. (Joint work with Jeffrey Hoffstein) (Received December 14, 2018)