1129-05-521 **Miaomiao Zhang*** (miaomiaozhang@gmail.com). *Efficient Cryptographic Construction from Redactable Precedence Graphs.*

We introduce a new family of (probability distributions over) labeled graphs: Redactable precedence graphs and propose a construction of a redactable precedence graph family based on multinomial distributions, and prove that, for properly chosen parameters, the expected size of a graph is linear.

Our interest in redactable precedence graphs is motivated by the problem of designing digital signature schemes that support redaction. Given a document containing n subdocuments, a precedence relationship is a connection between two or more subdocuments where a subdocument must appear before another in order for the document integrity to be kept intact. We describe how to use our new graph family to obtain efficient transparent redactable signature algorithms that hide the number and locations of redacted subdocuments.

Based on joint work with Stuart Haber and Bill Horne. (Received March 22, 2017)