Pairing-based Cryptography: Past, Present, and Future

Dan Boneh[⋆]

Stanford University, $\{$dabo$\}$@cs.stanford.edu

Abstract. While pairings were first introduced in cryptography as a tool to attack the discrete-log problem on certain elliptic curves, they have since found numerous applications in the construction of cryptographic systems. To this day many problems can only be solved using pairings. A few examples include collusion-resistant broadcast encryption and traitor tracing with short keys, 3-way Diffie-Hellman, and short signatures.

In this talk we survey some of the existing applications of pairings to cryptography, but mostly focus on open problems that cannot currently be solved using pairings. In particular we explain where the current techniques fail and outline a few potential directions for future progress.

One of the central applications of pairings is identity-based encryption and its generalization to functional encryption. While identity-based encryption can be built using arithmetic modulo composites and using lattices, constructions based on pairings currently provide the most expressive functional encryption systems. Constructing comparable functional encryption systems from lattices and composite arithmetic is a wonderful open problem. Again we survey the state of the art and outline a few potential directions for further progress.

Going beyond pairings (a.k.a bi-linear maps), a central open problem in public-key cryptography is constructing a secure tri-linear or more generally a secure n-linear map. That is, construct groups G and G_{T} where discrete-log in G is intractable and yet there is an efficiently computable non-degenerate n-linear map $e : G^n \to G_{\mathrm{T}}$. Such a construct can lead to powerful solutions to the problems mentioned in the first paragraph as well as to new functional encryption and homomorphic encryption systems. Currently, no such construct is known and we hope this talk will encourage further research on this problem.

[⋆] Supported by NSF, DARPA, AFOSR, Google, and Samsung.