

MANY CHEERFUL FACTS

presents

All good things come in pairs.

a talk by David Freeman

12:10 am - 1:00 on Wednesday, February 23th, in room
1015.

The use of bilinear pairings has recently become a hot topic in the field of cryptography. I will give a short overview of cryptographic pairings and discuss the important examples of the Weil and Tate pairings on elliptic curves. I will then describe three important applications: tripartite secret sharing, identity-based encryption, and short digital signatures. Along the way we will see what security properties a pairing must have for it to be useful in cryptography, and indicate why we think the elliptic curve pairings are good ones to use.

*I am the very model of a modern Major General,
I've information vegetable, animal, and mineral,
I know the kings of England, and I quote the fights historical
From Marathon to Waterloo, in order categorical;
I'm very well acquainted, too, with matters mathematical,
I understand equations, both the simple and quadratical,
About binomial theorem I'm teeming with a lot o' news,
With many cheerful facts about the square of the hypotenuse!*

- Gilbert & Sullivan $P \circ P$