

# Standard for Pairing based Cryptographic Techniques

1363.3

# IEEE1363.3

- ▶ Standard on Pairing Based Cryptographic Techniques
  - New stand-alone standard (not extension of 1363)
  
- ▶ Scope:

Specification of Identity-Based cryptographic techniques based on Pairings. Specification of Pairings, algorithms to compute the pairings, recommended elliptic curves and curve parameters. Class of computer and communications systems is not restricted.
  
- ▶ Volunteers:
  - Guido Appenzeller
  - Mike Scott (Algorithms)
  - Hovav Shacham (Pairings and Curves)

# History and Current Status

- ▶ Jan 12 Study Group Established
- ▶ April 18 PAR drafted by Study Group
- ▶ July 11 PAR approved by MSC (sponsoring body)
- ▶ Sep 22 Expected to be voted on by the IEEE Standards Board Meeting

Then the actual work starts...

# Submissions

## Proposed Structure:

- ▶ Post a call for submissions soon after vote
- ▶ Submissions start Oct 1<sup>st</sup>, 2005
  - Presenting ideas now is encouraged
  - We'll hear a first proposal tomorrow
- ▶ We accept submissions for 6 months (until March 30)
- ▶ A presentation to the IEEE group on submitted materials is encouraged (but not required)
- ▶ Submissions must be mailed to Editor/Chair and will be posted on the IEEE web site and mailing list

# Submission Areas

- ▶ Curves
  - Curve types
  - Weak curves/parameters
- ▶ Pairings
  - Pairings and how to compute them
- ▶ Algorithms
  - Encryption
  - Signatures?
  - Others Methods?
- ▶ Rule-of-thumb is to standardize about two of each
  - i.e. two types of curves, two encryption algorithms etc.

# Submissions

Submissions have to include:

- ▶ Description of the cryptographic technique
  - References are encouraged for background, the description should be understandable without the references.
- ▶ Claimed attributes and advantages of the technique
  - Working, reviewable implementations are a plus
- ▶ Security assessment and considerations
- ▶ Known limitations and disadvantages.
- ▶ Intellectual property issues.
  - Any patents or patent applications relating to the technique should be identified.
  - If the submission is accepted as part of the draft standard, a statement on licensing will be required, per IEEE policy.

# Criteria for selection

Relevant criteria will include:

- ▶ Performance
  - Number of primitives per operation
  - Execution speed on modern CPUs and embedded systems
- ▶ Security
  - Strength of proof of security
  - Amount of peer review of technique
- ▶ General Interest Level
  - Level of interest in the algorithms or primitives
  - Existing implementations

# Proposed Timeline

- ▶ Oct 2005 Call for submissions
- ▶ Apr 2006 Begin selection
- ▶ Oct 2006 Complete selection
- ▶ Apr 2007 First complete draft of standard