SM2: A Group of ECC Public Key Algorithms

Sean Shen

shenshuo@cnnic.cn

Xiaodong Lee

xl@cnnic.cn

What is it

- A group of ECC Public Key Algorithms includes: Basics & Terms, ECDSA, ECDH, Public Key Encryption
- Designed by Xiaoyun Wang, etc, before 2006
- Published in 2010
- Requested to be used in China in WLAN and some oth er communication scenarios
- Becomes industry standards in 2012.03
- Applied to multiple industry standards in 2012.11
- Will becomes National Standards soon

The draft

- draft-shen-sm2-ecdsa-00
  - Basics and Terms
  - ECDSA and Examples
- draft-shen-sm2-ecdsa-01
  - Basics and Terms
  - ECDSA, ECDH, Public Key Encryptions
  - All Examples

Some Statements about the draft

This document describes Public Key Algorithms based on elliptic curves which are invented by Xiaoyun Wang et al. These algorithms are published by Chinese Commercial Cryptography Administration Office for the use of electronic authentication service system, etc.

This document is mainly the translation of the algorithms published by Chinese Commercial Cryptography Administration Office for the convenience of IETF and IRTF community. The credit of designing the algorithms goes to the authors of the algorithms.

Where to find it

- http://www.oscca.gov.cn/News/201012/News_1198.
- Algorithms and Recommended parameters
- Unfornately in Chinese, that's why we do provide this draft

Next?

- Fix all the typos & mistakes
- Add the recommended parameters
- Build a website to provide all information related: algorithm, parameters, examples, implementations, attacks, comments & an swers, ...

Eventually

- Hope to make the algorithms public to th e community especially to IETF and IRTF
- Algorithms adopted as IETF Standards
- Applied to other IETF Standards which ne ed related algorithms, like DNSSEC

Thanks!