International Adoption of Chinese Cryptography Algorithms

The Implementation and Standardization Progress

Paul Yang
BaishanCloud / OpenSSL
Me…

- Architect at BaishanCloud, a startup cloud computing company
- OpenSSL Committer
Chinese Algorithms

• 5 major Chinese Cryptographic Algorithms
  • SM2, a public key algorithm (signature, key exchange and encryption schemes)
  • SM3, a hash function
  • SM4, a block cipher
  • SM9, an identity based encryption algorithm
  • ZUC, a stream cipher
Bouncy Castle

• Australian based open source project founded in 2000
• Provides APIs in Java and C#.Net languages
• APIs include basic cryptography services and more high-level APIs support certificate generation, TLS, secure MIME, and OpenPGP message handling.
• Development funded through donations and commercial support contracts.
• Home at: https://www.bouncycastle.org
• Code also mirrored at: https://github.com/bcgit
Bouncy Castle and Chinese Ciphers

• Bouncy Castle Java 1.6.0 (current release)
  • SM2
  • SM3
  • SM4

• Bouncy Castle C# .Net 1.8.3 (current release)
  • SM2
  • SM3

• SM4 for C# .Net is going to support in next release (1.8.4)
OpenSSL

• A very widely used SSL/TLS and cryptography library
  • Written in C language
  • But wrapped for many other programming languages
  • 20 years old now, founded in 1998…

• Typical usage
  • Combined with web servers to provide HTTPS services

• Latest release: 1.1.1
  • in September, 2018
  • A bundle of new features…
OpenSSL and Chinese Ciphers

• Started from last OpenSSL China tour
  • To make OpenSSL be recognized wider in China
• In OpenSSL 1.1.1
  • SM4
  • SM3
  • SM2
• ZUC is in review status
• SM9 has not started yet
What has not been done?

• No cipher suites for TLS protocols
  • Which makes it not possible to make ‘real’ TLS handshakes…
• No SM2 certificate support
  • OpenSSL only supports the ‘base’ SM2 algorithm
What’s next?

• Resolve the problems in previous slide…
• Support ZUC and SM9
• Make Chinese ciphers get more supported in other open source crypto libraries
  • Client side is also important, such as browsers…
Standardization Status

• ISO
  • SM2/SM9: ISO/IEC 14888-3:2016/DAmd 1

• 3GPP LTE
  • ZUC as 128-EEA3 and 128-EIA3

• TPM 2.0
  • SM2/SM3/SM4 (If I recall correctly…)

• ……
IETF

• Previous efforts in making IETF RFCs
  • draft-shen-sm2-ecdsa-02, 2014, CNNIC
  • draft-sca-cfrg-sm3-02, 2017, SCA/BaishanCloud/Ribose et al
  • draft-ribose-cfrg-sm4-10, 2017, Ribose et al
  • draft-sca-curdle-tls-sm34-0, 2018, BaishanCloud/Ribose et al
• Current progress…
  • Design new Chinese cipher suites for TLS 1.2 and TLS 1.3
  • Make new SM2 and other algorithm RFC drafts based on relevant ISO docs
    • SM2, SM3, SM4
    • SM9 and ZUC probably need to be addressed as well…
• Submit a new batch of drafts to several IETF WGs
  • Curdle
  • CFRG
OASIS KMIP

• KMIP
  • Key Management Interoperability Protocol
  • SM2/SM3/SM4 numeric IDs are assigned
  • Will be standardized soon
Next move...

- PCKS#11?
- CA/B Forum Baseline Requirement?
Thank you very much!

Paul Yang

Email: yang.yang@baishancloud.com
Github: @InfoHunter