Overview and Comparison of Open Source Cryptographic Libraries

Cong Chen
Yuqi Wang

Libraries

- Cryptlib;
- GNU Crypto;
- MatrixSSL;
- Mozilla NSS;
- NaCl;
- OpenCDK;
- OpenPGP SDK;
- WolfCrypt Embedded Crypto Engine.

Evaluation criteria

- Licenses ;
- Language;
- Operating system;
- Supported compilers;
- Cryptographic algorithms and key sizes;
- Support for random key generation;
- Performance of primitive cryptographic operations;
- Documentation and ease of use.

Licenses

- Free license
  - GPL
    - Cryplib;
    - GNU Crypto;
    - MatrixSSL;
    - WolfCrypt Embedded Crypto Engine.
  - MPL v2
    - Mozilla NSS.
  - BSD License
    - OpenPGP SDK.
- Charged license
  - Standard commercial license
    - Cryptlib;
    - MatrixSSL;
    - WolfCrypt Embedded Crypto Engine($5,000).

Language

- Written-in language
  - Language that the library used to build the source code;
- Supported language
  - Languages that the libraries can be used in projects.

Written-in language

- Java: GNU Crypto;
- C/C++: MatrixSSL;
- C: Cryptlib , Mozilla NSS, NaCl, OpenCDK, OpenPGP SDK, WolfCrypt Embedded Crypto Engine.

Supported language

- Java: Cryptlib, GNU Crypto;
- C++: Cryptlib, MatrixSSL , Mozilla NSS;
- C: Mozilla NSS, NaCl, OpenCDK,
  OpenPGP SDK,
  WolfCrypt Embedded Crypto Engine;
- Python: NaCl, Cryptlib;
- C# / .NET,Delphi, Visual Basic: Cryptlib.

Operating system

- Windows
  - Cryptlib;
  - GNU Crypto;
  - MatrixSSL;
  - Mozilla NSS;
  - OpenCDK;
  - OpenPGP SDK;
  - WolfCrypt Embedded Crypto Engine.
- Mac
  - MatrixSSL;
  - OpenCDK;
  - OpenPGP SDK;
  - WolfCrypt Embedded Crypto Engine.
- Linux/Unix
  - Cryptlib;
  - MatrixSSL;
  - Mozilla NSS;
  - NaCl;
  - OpenCDK;
  - OpenPGP SDK;
  - WolfCrypt Embedded Crypto Engine.

Compilers

- GNU compiler collection
  - MatrixSSL;★
  - 64-bit OpenCDK;★
  - OpenPGP SDK;★
  - WolfCrypt Embedded Crypto Engine.★
- GNU Compiler for the Java
  - GNU Crypto.
- All compilers
  - Cryptlib;★
  - Mozilla NSS;★
  - 32-bit OpenCDK;★
  - NaCl.

★ Using cross-compilers

CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES

Catagory

- Public-key encryption algorithms;
- Secret-key algorithms;
- Hash function;
- MAC.

Step 1 :Collect data

- Mozilla NSS as an example.

Secret Key	Maximum key size (bits)
DES	56/112/168
Triple-DES	56/112/168
AES	128/192/256
ECDH	571 for GF(2^m), 521for GF(p)
RC2	Variable
RC4	Variable

Hash	Block size (bits)
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512
MD-2	128
MD-5	128

Public key	Maximum key size (bits)
Diffie-Hellman	2236
RSA	8192
DSA	1024
ECDSA	571 for GF(2^m), 521for GF(p)
ECC	ECC code not compiled by default

Message Authentication	Block size (bits)
HMAC SHA-1	160
HMAC SHA-224	224
HMAC SHA-256	256
HMAC SHA-384	384
HMAC SHA-512	512

Step 1 :Collect data

- NaCl's crypto-box.

Public-key cryptography: Authenticated encryption						
crypto_box	Public key	Secret key	Nonce	Zero	Boxzero	Beforenm
crypto_box_nistp256aes256gcm	512	256	64	256	0	256
crypto_box_curve25519xsalsa20poly1305	256	256	192	256	128	256

Secret-key cryptography: Authenticated encryption				
crypto_secretbox	Key	Nonce	Zero	Boxzero
crypto_secretbox_aes256gcm	256	64	256	0
crypto_secretbox_xsalsa20poly1305	256	192	256	128

Step 1 :Collect data

- OpenCDK
  - The main purpose of OpenCDK is to handle OpenPGP packets and to use basic operations, so the library doesn’t contain any real cryptographic code.

Step 2: Summary all the algorithms

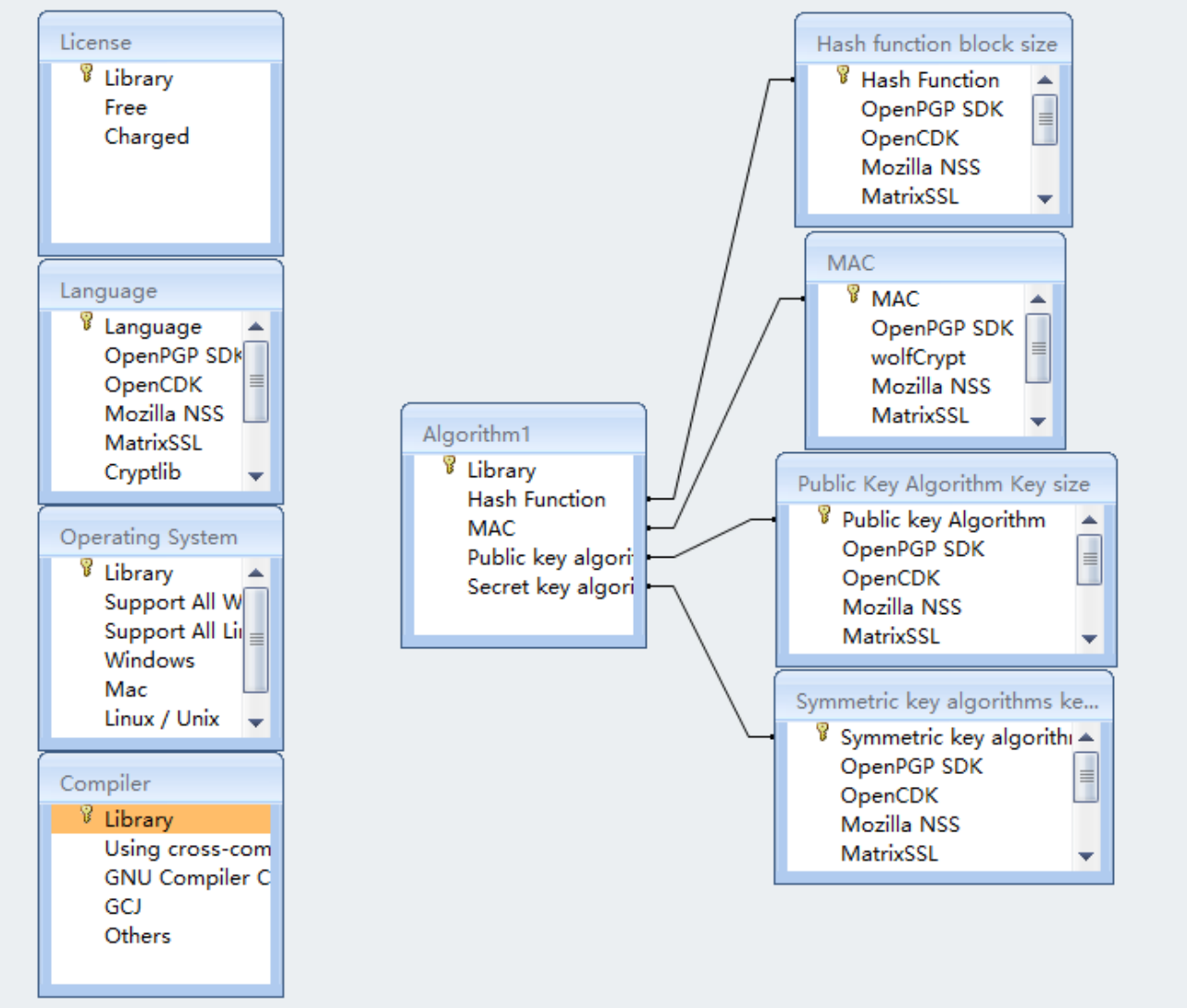
- Public-key encryption algorithms as an example

  - DHE/ECDHE;
  - Diffie-Hellman;
  - DSA(DSS);
  - ECC;
  - ECDH;
  - ECDSA;
  - EDH;
  - Elgamal;
  - NTRU;
  - RSA;
  - SRP6.

Step 3: Design forms

Public key Algorithm	Cryptlib	GNU Crypto	NaCl	MatrixSSL	Mozilla NSS	OpenCDK	OpenPGP SDK	wolfCrypt
DHE/ECDHE								
Diffie-Hellman								
DSA(DSS)								
ECC								
ECDH								
ECDSA								
EDH								
Elgamal								
NTRU								
RSA								
SRP6								

Step 4: Database



Step 4: Database

Algorithm	Cryptlib	GNU Crypt	MatrixSSL	Mozilla NS	NaCl	OpenCDK	OpenPGP SDK	wolfCrypt
Hash Function	MD2 MD4 MD5 RIPEMD-160 SHA-1 SHA-2 / SHA-256	MD2 MD4 MD5 RIPEMD128 RIPEMD-160 SHA-160(SHA-256, SHA-	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 MD-5	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 MD-2 MD-5	crypto_hash box		SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	MD-2 MD-4 MD-5 SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
Mac Function	HMAC MD-5 HMAC SHA-1 HMAC SHA-256 HMAC RIPEMD-160	HMAC MD-2 HMAC MD-4 HMAC MD-5 HMAC-RIPEMD128 HMAC-RIPEMD160 HMAC SHA-1	HMAC SHA-1 HMAC SHA-224 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512	HMAC SHA-1 HMAC SHA-224 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512	crypto_box		HMAC SHA-1 HMAC SHA-224 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512	HMAC PBKDF2 PKCS#5
Public Key	Diffie-Hellman DSA ECDSA ECDH Elgamal RSA	DH DSS (DSA) RSA SRP6	Diffie-Hellman RSA DHE/ECDHE ECC	Diffie-Hellman RSA DSA ECDSA ECC	crypto_box		RSA DSA	RSA, DSS, DH, EDH, NTRU, DSA
Secret Key	AES, Blowfish, CAST-128, DES, Triple DES, IDEA, RC4, RC5, Skipjack	AES ANUBIS ARCFOUR (RC4) BLOWFISH DES KHAZAD RIJNDAEL	AES AES-GCM PSK	DES Triple-DES AES ECDH RC2 RC4	crypto_secretbox		Triple-DES TECB, TCBC, TCFB AES-128 AES-192 AES-256 ECB, CBCand CFB128	AES (CBC, CTR, GCM, CCM), Camellia, DES, 3DES, ARC4, RABBIT, HC-128, ECC

Step 4: Database

- Example of public-key algorithms

Public Key Algorithm Key size

Public k	Cryptlib	GNU Crypt	NaCl	Matri	Mozilla NSS	OpenCD	OpenPGP S	wolfCryp
DHE/ECDHE				1024 /				
Diffie-Hel	4096	Set by user		1024	2236			Set by us
DSA(DSS)	4096	512/ 768/ 1			1024		1024	Set by us
ECC				192	ECC code not compiled			up to 512
ECDH	521							up to 512
ECDSA	521				571 for GF(2^m), 521f			
EDH								Set by us
Elgamal	4096							
NTRU								Set by us
RSA	4096	Set by user		1024	8192		2048 (max 4	4096
SRP6		512/ 640/76						

Step 4: Database

- Example of searching

Support for random key generation

- PRNG (Pseudo-random number generator)
  - Cryptlib;
  - GNU Crypto;
  - Mozilla NSS;
  - NaCl;
  - OpenPGP SDK;
  - WolfCrypt Embedded Crypto Engine.
- ARC4 (Alleged Rivest Cipher 4)
  - GNU Crypto;
  - NaCl.
- Built-in randomness sources
  - Cryptlib;
  - MatrixSSL;
  - Open CDK.

Performance

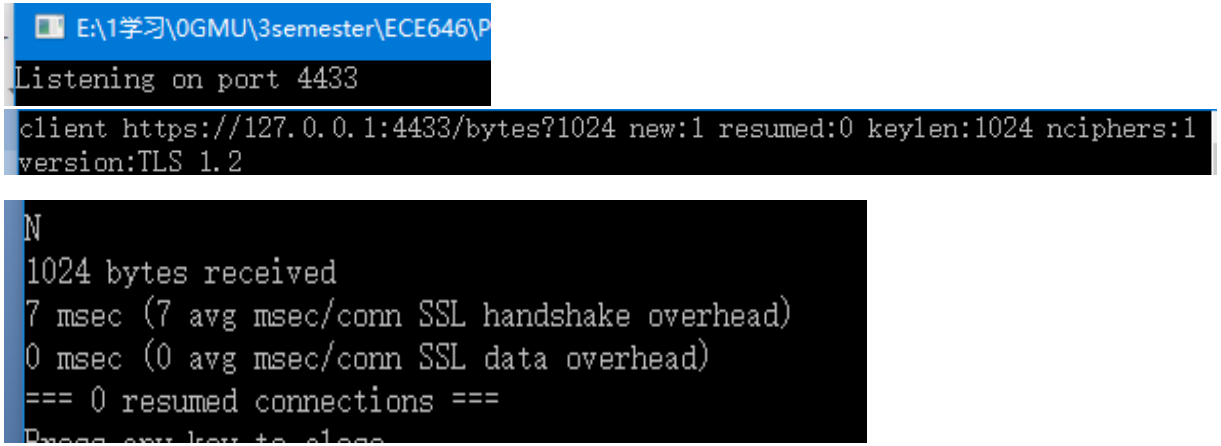
- Attack
  - Fixed
    - Phishing attack: Cryptlib;
    - Heartbleed attack: MatrixSSL;
    - Bleichenbacher attack on PKCS#1: Mozilla NSS;
    - MITM attack: OpenPGP SDK;
  - Not fixed yet
    - Timing attack: NaCl.

Performance

- Speed
  - NaCl and wolfCrypt Embedded Crypto Engine are faster.
- Size
  - Large (over 150M): OpenCDK, OpenPGP SDK;
  - Average (around 20M): Cryptlib, GNU Crypto;
  - Small (less than 10M): MatrixSSL, wolfCrypt Embedded Crypto Engine.

Performance

- MatrixSSL



Documentation and Ease of use

- **Documentation**
  - Rich manual, rich research paper: MatrixSSL
  - Rich research paper: Cryptlib, Mozilla NSS, OpenPGP SDK
- **Ease of use**
  - Easy: Cryptlib, MatrixSSL, NaCl,
    wolfCrypt Embedded Crypto Engine
  - Relatively hard: OpenCDK, OpenPGP SDK

Reference

- [1] Website Redesign Company. (Oct. 2010). cryptlib. Available: http://www.cryptlib.com/downloads/manual.pdf Accessed: Oct. 26 2015
- [2] Peter Gutmann. cryptlib Security Toolkit v3.4. Available: http://www.cryptlib.com/ Accessed: Oct. 26 2015
- [3] Free Software Foundation, Inc. The GNU Crypto project Available: https://www.gnu.org/software/gnu-crypto/ Accessed: Oct. 26 2015
- [4] INSIDE Secure Corp. MatrixSSL - Open source embedded SSL. Available: http://www.matrixssl.org/ Accessed: Nov. 9 2015
- [5] INSIDE Secure Corp. (2013). MatrixSSL 3.7 APIs. Available http://www.matrixssl.org/doc/MatrixSSL_API.pdf Accessed: Nov. 9 2015
- [6] Computer Aided Cryptography Engineering. NaCl: Networking and Cryptography library. Available http://nacl.cr.yp.to/ Accessed: Nov. 9 2015
- [7] D. J. Bernstein et.al. (n.d.). The security impact of a new cryptographic library. [Online]. Available: http://cr.yp.to/highspeed/coolnacl-20120725.pdf Accessed: Oct 17 2015
- [8] J. Callas et. al. "OpenPGP Message Format". RFC: 2440, Nov, 1998. [Online]. Available: https://www.ietf.org/rfc/rfc2440.txt Accessed: Nov 22th 2015
- [9] Network Associate. (1999). *PGP Software Developer's Kit User's Guide.* (v1.17). [Online]. Available: ftp://ftp.pgpi.org/pub/pgp/sdk/PGPsdkUsersGuide.pdf Accessed: Oct 17, 2015
- [10] wolfSSL Inc.wolfCrypt Embedded Crypto Engine. Available https://www.wolfssl.com/wolfSSL/Products-wolfcrypt.html Accessed: Oct 17, 2015
- [11] U. Kumar et al. (Apr 16th, 2015). Comparative Analysis of Cryptography Library in IoT. [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1504/1504.04306.pdf [Oct 17, 2015]
- [12] Berkeley DB. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/w/index.php?title=Berkeley_DB&redirect=no#Sleepycat_License Accessed: Dec. 12 2015

Reference

- [13] Various Licenses and Comments about Them. (n.d.). *GNU Operating System*. Available: http://www.gnu.org/licenses/license-list.en.html Accessed: Dec 11 2015
- [14] Mozilla Developer Network and individual contributors. Network Security Services. Available: https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS Accessed: Nov. 9 2015
- [15] Vidya G. (July 15th, 2013). Forensic Analysis of PGP-Encrypted Files. [Online]. Available: http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Vidya%20G_Forensic%20analysis%20of%20PGP-encrypted%20files_2013.pdf [Oct 17, 2015]
- [16] C. Marshall, R. S. Naffah.(2003, Nov.9). Programming with GNU Crypto. [Online]. Available: http://www.gnu.org/software/gnu-crypto/manual/gnu-crypto.pdf Accessed: Oct 17 2015
- [17] INSIDE Secure Corp. (2013). MatrixSSL Developer's Guide, v3.7. Available http://www.matrixssl.org/doc/MatrixSSL_DeveloperGuide.pdf Accessed: Nov. 9 2015
- [18] WolfSSL. *Chapter 10: wolfCrypt (formerly CTaoCrypt) Usage Reference*. [Online]. Available: https://www.wolfssl.com/wolfSSL/Docs-wolfssl-manual-10-wolfcrypt-usage-reference.html [Oct 17, 2015]
- [19] The GNU Ada Development Environment. GNAT User's Guide for Native Platforms v 6.0.0. (Nov. 18, 2015). chpt. 8.3.1.3 [Online]. Available: https://gcc.gnu.org/onlinedocs/gnat_ugn/ Dec. 1 2015
- [20] Elliptic Curve Digital Signature Algorithm. (n.d.).*Wikipedia*. Available: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm Accessed: Oct 17 2015
- [21] D. Johnson, A. Menezes, S. Vanstone. (n.d.). The Elliptic Curve Digital Signature Algorithm (ECDSA). [Online]. Available: http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf Accessed: Nov. 9 2015
- [22] Don B. Johnson. (Oct. 1997). ANSI X9.F.1 Cryptographic Standards. [Online]. Available: http://csrc.nist.gov/nissc/1997/proceedings/761slides.pdf Accessed: Dec. 12 2015

Thank you!