Proposal of addition of new cipher suites to TLS to support Camellia, EPOC, and PSEC

Shiho Moriai
shiho@sl.ntt.co.jp
NTT Laboratories
128-bit Block Cipher

Camellia

Kazumaro Aoki*  Tetsuya Ichikawa†
Masayuki Kanda*  Mitsuru Matsui†
Shiho Moriai*  Junko Nakajima†
Toshio Tokita†

* NTT
† Mitsubishi Electric Corporation
What’s Camellia?

- **128-bit Block Cipher**
  - Jointly developed by NTT and Mitsubishi
  - Designed by experienced cryptanalysts and programmers

- **Supports 128-, 192-, 256-bit keys**
  - Same interface as Advanced Encryption Standard (AES)
  - Offer more security against exhaustive key search
Design Goals

- High level of security
  - State-of-the-art cipher analysis technology

- Efficiency on multiple platforms
  - Software: 8-bit, 32-bit, 64-bit processors
  - Hardware: compact and high-performance
Software Performance (128-bit keys)

- On a Pentium III
  - 309 cycles/block (Assembly) = 469 Mbps (1.13 GHz)
- Much faster than DES
- Comparable speed to the AES finalists

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encryption speed on P6 [cycles/block]</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC6</td>
<td>229</td>
</tr>
<tr>
<td>Rijndael</td>
<td>238</td>
</tr>
<tr>
<td>Twofish</td>
<td>288</td>
</tr>
<tr>
<td>Camellia</td>
<td>309</td>
</tr>
<tr>
<td>Mars</td>
<td>312</td>
</tr>
<tr>
<td>Serpent</td>
<td>759</td>
</tr>
</tbody>
</table>

*The programs are written in assembly language by Aoki, Lipmaa, and Osvik. Each figure is the fastest as far as we know.*
Hardware (128-bit keys)

- ASIC (0.35µm CMOS)
  - Small Size Hardware 11K Gates
    - Smallest among existing 128-bit block ciphers
  - High Performance Hardware

<table>
<thead>
<tr>
<th></th>
<th>Area [Kgates]</th>
<th>Throughput [Mbit/s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>MARS</td>
<td>2,936</td>
<td>226</td>
</tr>
<tr>
<td>RC6</td>
<td>1,643</td>
<td>204</td>
</tr>
<tr>
<td>Rijndael</td>
<td>613</td>
<td>1,950</td>
</tr>
<tr>
<td>Serpent</td>
<td>504</td>
<td>932</td>
</tr>
<tr>
<td>Twofish</td>
<td>432</td>
<td>394</td>
</tr>
<tr>
<td>Camellia</td>
<td>273</td>
<td>1,171</td>
</tr>
<tr>
<td>DES*</td>
<td>54</td>
<td>1,161</td>
</tr>
</tbody>
</table>

*DES is a 64-bit block cipher.

The above data (except Camellia) are presented by Ichikawa et al. at the 3rd AES conference.
Camellia provides strong security against differential and linear cryptanalysis.

Moreover, Camellia was designed to offer security against other advanced cryptanalytic attacks:
- truncated differential attacks,
- higher order differential attacks,
- interpolation attacks,
- related-key attacks, ...
For more information...

Camellia Home Page

http://info.isl.ntt.co.jp/camellia/
- Specification & Sample code
- Technical papers on design rationale, performance, software implementation techniques, and security evaluation
- Internet-Draft on description of Camellia will be available soon!
Public Key Algorithms

EPOC and PSEC

Tatsuaki Okamoto
Shigenori Uchiyama
Eiichiro Fujisaki

NTT

2000.8.1. 48th IETF Meeting TLS
Provable Security of Public Key Algorithms

- Flaw in RSA with PKCS #1 Ver.1
  - Importance of security against adaptively chosen ciphertext attacks

- EPOC & PSEC
  - Developed by Okamoto et al. (NTT)
  - Provably secure under the random oracle model in the strongest sense (i.e., non-malleable against adaptively chosen ciphertext attacks)
EPOC (Efficient Probabilistic Public-Key Encryption Scheme)

- **Novelty**
  - Essentially different from any other previous schemes including RSA-Rabin and Diffie-Hellman

- **Security**
  - Provably as secure as factoring in the strongest sense

- **Efficiency**
  - Compared with RSA (PKCS#1 Ver.2) with small $e (2^{16}+1)$, encryption speed is slower, but decryption speed is faster.
PSEC (Provably Secure Elliptic Curve Encryption Scheme)

- **Security**
  - Provably as secure as elliptic-curve Diffie-Hellman problem in the strongest sense

- **Efficiency**
  - Almost as efficient as most common ECC, elliptic-curve ElGamal (Diffie-Hellman) scheme
Toward International Standards

- EPOC
  - IEEE P1363a \((\text{royalty free if selected})\)

- Camellia
  - ISO/IEC J TC 1/SC27
  - NESSIE (New European Schemes for Signature, Integrity, and Encryption)
Sample Code

- Camellia
  - http://info.isl.ntt.co.jp/camellia/
- EPOC & PSEC
  - http://www.nttmcl.com/sec/
Conclusion

- Camellia is a 128-bit block cipher with high security and performance
  - suitable for bulk encryption
- PSEC and EPOC are public-key algorithms with provable security and efficiency
  - suitable for key exchange and authentication
**Conclusion (Cont.)**

- Add them to Transport Layer Security!!

```c
enum { null, rc4, rc2, des, 3des, des0, idea, ..., camellia } BulkCipherAlgorithm

enum { rsa, diffie-hellman, epoc, psec } KeyExchangeAlgorithm

enum { anonymous, rsa, dsa, epoc, psec } SignatureAlgorithm
```