Understanding Public-Key Performance

Matthew Short Matt.Short@Freescale.com
Geoffrey Waters G.Waters@Freescale.com

Public-key operations are used in a wide range of networking protocols to provide authentication, non-repudiation, and private-key exchange. All Freescale's security co-processors, and several PowerQUICC™ communications processors with integrated security engines (SEC) offer public-key acceleration via a public-key execution unit (PKEU). The purpose of this white paper is to assist the user in understanding the performance they are likely to achieve when off-loading public-key operations to the PKEU.

While 'connections per second' seems like a straightforward metric, a connections-per-second benchmark for SSL, IKE, or other public key based secure session establishment protocols introduces protocol and network overhead which is often neglected by security vendors. Aside from these protocol overheads, public-key performance is also dependent on the size of the operands. In client/server applications, the private key (modulus) is often large, and the public key (exponent) is small. In peer-to-peer session establishment, the public and private keys are typically the same size. Unless a vendor explains how they account for protocol overheads and operand size differences, a connections-per-second comparison is meaningless.

Freescale products are used in a wide range of applications, and this white paper is offered to provide users with public-key performance metrics applicable to the full range of Freescale products with public-key acceleration. The assumptions used in generating the performance figures in Table 1 are listed below.

- A full IKE exchange, SSL handshake, or X.509 certificate verification introduces protocol overhead that is outside of the control of the PKEU. Consequently, Freescale quotes execution time for only the most common underlying function, RSA sign/verify.
- There is no set size for an RSA modulus or exponent, but some sizes and benchmarks are more common. Table 1 shows the modulus = exponent benchmark, and the large private-key (modulus), small public-key (exponent) benchmark.
- Modulus and exponent size are generally independent of the number of users, and are dictated by the application and security policy of an organization. 1024 bit keys are a common default.

- RSA sign/verify time is measured from the time the PKEU has loaded its operands to the time it signals DONE. CPU overhead and movement of the operands into the PKEU are not considered, however these overheads are negligible for public-key operations, as compared to private-key encryption/decryption.

Table 1 shows the performance of the public-key execution unit at various frequencies.

Table 1. RSA Performance [milliseconds]

Measurement Point	33 MHz	50 MHz	66 MHz	83 MHz	100 MHz	133 MHz	166 MHz	333 MHz
512 bit modulus 512 bit exponent	8.09 [ms]	5.34 [ms]	4.05 [ms]	3.22 [ms]	2.67 [ms]	2.01 [ms]	1.61 [ms]	0.80 [ms]
512 bit modulus 3 bit exponent	0.43 [ms]	0.29 [ms]	0.22 [ms]	0.17 [ms]	0.14 [ms]	0.11 [ms]	0.09 [ms]	0.04 [ms]
1024 bit modulus 1024 bit exponent	54.71 [ms]	36.11 [ms]	27.35 [ms]	21.75 [ms]	18.05 [ms]	13.57 [ms]	10.88 [ms]	5.42 [ms]
1024 bit modulus 3 bit exponent	1.48 [ms]	0.97 [ms]	0.74 [ms]	0.59 [ms]	0.49 [ms]	0.37 [ms]	0.29 [ms]	0.15 [ms]
2048 bit modulus 2048 bit exponent	406.50 [ms]	268.29 [ms]	203.25 [ms]	161.62 [ms]	134.14 [ms]	100.86 [ms]	80.81 [ms]	40.28 [ms]
2048 bit modulus 3 bit exponent	5.40 [ms]	3.56 [ms]	2.70 [ms]	2.15 [ms]	1.78 [ms]	1.34 [ms]	1.07 [ms]	0.53 [ms]

These execution times can easily be converted into 'number of connections per second', (1/execution time = ops/sec), with the understanding that generation of protocol messages, transmission of messages, and receipt of responses are not included. The deterministic portion of connection set-up is the RSA sign/verify execution time (in milliseconds), which is provided.

Conclusion

Public-key operations are some of the most computationally intensive functions occurring in networks today. By off-loading these functions to a dedicated public-key accelerator, Freescale security solutions complete RSA sign/verification of protocol messages 500–1000x faster than the same function in software, and significantly reduce CPU use during secure session establishment.

THIS PAGE INTENTIONALLY LEFT BLANK

How to Reach Us:

Home Page:
www.freescale.com

email:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
(800) 521-6274
480-768-2130
support@freescale.com

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Technical Information Center
3-20-1, Minami-Azabu, Minato-ku
Tokyo 106-0047 Japan
0120 191014
+81 3 3440 3569
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
(800) 441-2447
303-675-2140
Fax: 303-675-2150
LDCForFreescaleSemiconductor@
hibbertgroup.com

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters which may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.