RSA vs. ECC Comparison for Embedded Systems

Introduction

Author: Kerry Maletsky

Modern cryptographic protocols increasingly use asymmetric algorithms such as RSA and ECC because of their flexibility and enhanced ability to manage keys. Developed in the late '70s, the Rivest, Shamir and Adelman algorithm (RSA) has become the algorithm of choice for internet security. Elliptic Curve Cryptography (ECC), which was first proposed in the '80s, is becoming more widely used for many reasons. There are important differences between the two which warrant a careful comparison.

Security Matters

The level of security in systems is a primary concern. Most cryptographic experts recommend that current systems offer at least 128 bits of security. This does not represent the key length. Security comes from the combination of the specific algorithm and its key length. For example, it is generally thought that 128 bits of security can be achieved with 128-bit AES keys, 256-bit Elliptic Curve keys and 3072-bit RSA keys. If implementation issues are ignored, then these algorithms with the specified key lengths will generally have the same level of security. See www.keylength.com[(1)] for recommendations from various sources. Typical RSA implementations currently employ 1024-bit or 2048-bit keys, yet both are less secure than AES-128.

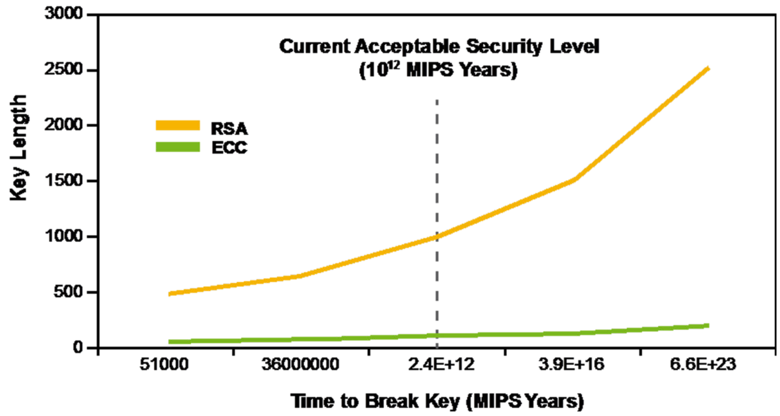
Table 1. Security Comparison for Various Algorithm Key Size Combinations (Source: NSA)[(5)]

Security Bits	Symmetric Encryption Algorithm	Minimum Size (Bits) of Public Keys	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

Key lengths generally increase over time as the computation available to attackers continues to increase. This is a manifestation of the cryptographic arms rate. Some experts suggest that AES-256 be employed for data encryption rather than the prior accepted AES-128 protocol. If elliptic curves are used for the key management (i.e., the encryption/decryption session key) of an AES-256 session, then a 512-bit elliptic curve session key is required (see Table 1). To achieve the same level of security with RSA encryption, 15,360-bit keys are required, which is computationally infeasible in embedded systems today. This stark contrast between the feasibility of ECC over RSA indicates that ECC is the algorithm of the future for embedded systems.

Algorithm security is irrelevant if an attacker can obtain the keys via other methods. This point cannot be emphasized enough. Security starts and ends with how well the keys are protected. In addition to poor key storage, weak or faulty algorithm implementations, bad random number generation, and/or aggressive attacks on end point systems can also degrade security.

Figure 1. RSA and ECC Performance[(6)]



This chart presents what key lengths of each algorithm provide a level of security measured in time in MIPS-years to break the security. This illustrates that ECC is more efficient.

Performance Anxiety

When it comes to performance at 128-bit security levels, RSA is generally reported to be ten times slower than ECC for private key operations such as signature generation or key management. The performance disparity expands dramatically at 256-bit security levels, where RSA is 50 to 100 times slower. RSA's key generation is also very slow compared to ECC's key generation, with the RSA's being 100 to 1000 times slower. However, this may or may not be a significant consideration in systems that generate keys infrequently. It does matter for certain protocols or policies that require more frequent key generation.

Public key signature validation is generally faster with RSA compared to ECC, which can provide a benefit.

Bandwidth

When it comes to network bandwidth, the main concern relates to the symmetric algorithm used for message encryption and Message Authentication Coding (MAC) for integrity checking (this is unrelated to the choice of RSA versus ECC). Smaller embedded systems may start sessions more frequently, or the asymmetric authentication may be a larger percentage of the overall traffic and the size of the keys and signatures can make a difference. At the 128-bit security level, public keys and signatures are six times larger for RSA. Private keys are 12 times larger for RSA compared to ECC, at the 128-bit security level. The key size generally has no impact on performance, but size does matter when it comes to the cost of secure storage of the keys.

Government and Industry Standard Recommendations

Based upon the trade-offs noted earlier, there is an almost endless list of new standards that are mandating the use of ECC. A small selection is noted below:

- **ZigBee Networking Standards** – This standard includes the use of asymmetric algorithms for authentication and key management and specifies Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic-curve Diffie–Hellman (ECDH) as the algorithm of choice. See "Securing Ad Hoc Embedded Wireless Networks with Public-Key Cryptography".[(2)]
- **Security Module PP Standards** – The Federal Office for Information Security in Germany, Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI, has published a set of standards for energy metering gateway security, which specifies elliptic curves as the authentication algorithm. See "Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)".[(3)]
- **Intelligent Transportation Systems (ITS) Standards** – This U.S. Department of Transportation program documents standards for the automotive industry to include elliptic curves as the algorithm of choice for Vehicle-Vehicle communication security. See "Low-Latency ECDSA Signature Verification – A Road Towards Safer Traffic".[(4)]

- **Commercial National Security Algorithm (CNSA) Suite** – This U.S. National Security initiative publishes a set of standard algorithms approved for use in non-defense applications called *"Commercial National Security Algorithm Suite"*. This set of standards replaces the *"Suite B Cryptography Standards"*, previously specified by the US Government.[5]

Conclusion

Due to security issues, most new cryptographic protocols are moving away from RSA to elliptic curves. This transition is expedited in the embedded space because the ECC cost/performance benefits are quickly realized.

References

1. BlueKrypt – "Cryptographic Key Length Recommendation", 2015.
2. Mitch Blaser – "Securing Ad Hoc Embedded Wireless Networks with Public-Key Cryptography", 2006.
3. Bundesamt für Sicherheit in der Informationstechnik – "Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)", 2014.
4. Miroslav Knežević, Ventzislav Nikov, and Peter Rombouts – "Low-Latency ECDSA Signature Verification – A Road Towards Safer Traffic", 2014.
5. National Security Agency – "Commercial National Security Algorithm Suite", 2015.
6. M. Alimohammadi and A. A. Pouyan – "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET", 2014.

Revision History

Revision	Date	Description
A	04/2020	Original release of this document. This document replaces Atmel – 8951A – 07/2015.

The Microchip Website

Microchip provides online support via our website at http://www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to http://www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with

Trademarks

ISBN: 978-1-5224-5997-2

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit http://www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: http://www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820