SHORT ECC
A Lightweight Security Approach for Wireless Sensor Networks

Anna Sojka, Krzysztof Piotrowski and Peter Langendoerfer
IHP GmbH, Im Technologiepark 25, Frankfurt Oder, Germany

Keywords: Elliptic curves cryptography, Wireless sensor networks.

Abstract: This paper presents our ongoing work towards a new lightweight security approach for Wireless Sensor Networks. Applying several changes in the standard Elliptic Curve Cryptography parameter sets and algorithms we get a public/secret key hybrid with a reasonable security level and much shorter key sizes. Here we present the main idea, the algorithms together with the initial security analysis and the directions for the future research.

1 INTRODUCTION

The popularity of the Wireless Sensor Networks (WSN) grows rapidly. A WSN consists of small and low cost devices with constrained computational and energy resources–the sensor nodes. The wide spectrum of their applications starts with the most popular ones, like habitat or nature monitoring, and goes beyond to more demanding applications in military or security area, like monitoring of the firefighters (Freie Universitaet Berlin, 2008). A great number of these applications applies to areas that require discretion, for example in health monitoring. Sometimes the deployment of sensor nodes is random, changeable or easily accessible. Taking all these aspects into consideration it is clear that in many cases the transmition and the storage of data in WSN should be secured.

In (Piotrowski, 2006), the authors show that the energy needed for transmitting a single bit of information is equal to the energy needed by the microcontroller for several hundred or even thousand clock cycles of computation. The standard Public Key Cryptography security approaches are computationally very expensive. In the same paper the authors show that the generation or verification of a digital signature using the ECC P160 curve proposed by NIST (NIST, 2010) requires at least one order of magnitude more energy than sending it over the radio. The Secret Key Cryptography mechanisms are less expensive and in the case of AES 128 the encryption or decryption costs around the same amount energy as sending of a single block (Piotrowski, 2006) (SIC, 2009). The above mentioned numbers are given for the TmoteSky (Moteiv, 2006) node hardware platform equipped with the MSP430F1611 (Texas Instruments, 2009) microcontroller and a cc2420 (Texas Instruments, 2008) transceiver, both from Texas Instruments.

In this paper we present our ongoing work on new techniques for securing the data in WSN by using a modified EC Cryptosystem. In our approach we target at using curves with keylength between 32 and 64 bits, so usually recognized as non-secure. The changes applied to the parameter set–some public parameters become private–cause the Short Elliptic Curve (SEC) Cryptosystem to become a Public/Private Key Cryptography hybrid, but also causes the method to be very efficient. The efficiency advantages include reduction of the computational effort, but also reduction of the data block size, and thus reduction of energy needed for the transmition of the results. The security strength cannot be compared to the one delivered by standard EC Cryptosystems, but our preliminary analysis shows that breaking the security needs a huge storage capacity on the attacker side or quite expensive searches. Additional mechanisms, like using several parameter sets and switching between them, or frequent changes of the parameter set helps to avoid attacks on a statistical basis and provide even more security on the cost of the increased management overhead.

In this paper we introduce the idea, together with an initial analysis of its correctness. Since this is ongoing work, there is still room for tests, improvements and further research.

The rest of the paper is structured as follows.

Sojka A., Piotrowski K. and Langendoerfer P. (2010).
SHORT ECC - A Lightweight Security Approach for Wireless Sensor Networks.
In *Proceedings of the International Conference on Security and Cryptography*, pages 304-308
DOI: 10.5220/0002983003040308

The next section provides more information about the changes we applied to the standard ECC. Then we talk about the security analysis of our approach. The paper closes with the description of our future research directions.

2 SHORT ELLIPTIC CURVES

In this section we describe the SEC cryptosystem in detail.

2.1 Notation

In the rest of our paper we will use the following symbols:

- $\mathbb{F}_q$ - a finite prime field
- $E(\mathbb{F}_q)$ - an elliptic curve over field $\mathbb{F}_q$
- (x,y), where $x,y \in \mathbb{F}_q$ - a point on the elliptic curve
- $\mathcal{O}$ - the point at infinity
- $P = (x_P, y_P)$ - a base point on the elliptic curve
- p, where $pP = \mathcal{O}$ - order of the point P
- $\#E = n$ - order of the elliptic curve
- (k,Q) - a key pair , where the private key $k \in [0,p]$ and the public key is $Q = kP$
- $< P >$ - cyclic group of points generated by P

2.2 SEC based Cryptosystem

As Short Elliptic Curves (SEC) we consider elliptic curves over 32 to 64-bit finite prime fields. Standard elliptic curves are based on prime fields with an order at least twice that long (minimum 128-bits). Short curves are unsafe, if used with standard ECC protocols. Knowing all the public parameters, finding discrete logarithms, i.e., breaking the security system using such a small group takes only a few seconds on a standard PC. SEC based cryptosystem has the following features:

- It provides security means for a trusted group of participants sharing the same SEC parameters.
- It uses standard ECC in a layer which manages the distribution of SEC parameters (together with an algorithm for generating the chain of SEC or the set of SEC with the method for choosing valid SEC) to the new members of the group. After that the new group participant is able to manage the SEC parameters and change them if necessary.
- Encryption and digital signatures within the group are performed using SEC.
- To improve the security, one SEC setting is valid for a defined period of time only, after which all the group members generate the new SEC parameters and switch to them. Another option is to have a precomputed set of SEC and to switch between them according to some algorithm. Each group member generates the key pair for the new SEC. Public key is encrypted using previously valid elliptic curve and distributed to trusted group members.
- Compression for all transmitted SEC points is used. It reduces the amount of transmitted data and additionally improves the security.

2.3 Generation of a SEC

Generation of the new SEC parameters may be done by each node independently. Each node should get the same SEC parameters, so the generation process on each node needs to be synchronized and the new parameters do not need to be distributed. Only the public key of each node has to be broadcasted in an encrypted form using for example, the previous SEC. The general procedure of generation the SEC parameters from scratch is described below.

First, a prime number q has to be chosen to be the order of the finite field. Then the two integers $a,b \in \mathbb{F}_q$ that are the coefficients in the elliptic curve equation are to be determined. Next steps are to find the order of E, to choose a base point and to find its order.

To prevent from Pohlig-Hellman attack (Blake, 2000) it is necessary that the order of the base point is the largest possible prime integer. The ideal solution is to find a point which generates all the points on the curve E and has a prime order, equal to the curve order.

Lagrange's theorem says (Blake, 2000) that the order of an arbitrarily chosen group element $P \neq \mathcal{O}$ divides the order of the group. Thus, when a curve has a prime order n, there are only two possible orders of points on the curve: 1 and n, and since $1P = P \neq \mathcal{O}$, the only possible order of any point P is n. The Hasse's theorem (Koblitz, 1998) brings very useful information about the interval in which to look for the curve order and in the above mentioned case it is also the order of the base point. This theorem says that for an elliptic curve E over a finite field $\mathbb{F}_q$ the order of $E(\mathbb{F}_q)$ satisfies

$$q+1-2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q+1+2\sqrt{q} \qquad (1)$$

To find the curve order in this interval we proceed as follows:
Let $P = (x,y)$ be randomly chosen point on E and let

$$Q = (q+1+2\sqrt{q})P \qquad (2)$$

The next step is to find a second point $R = zP$, where $z \neq (q+1+2\sqrt{q})$ and $R = Q$. Since $Q - R = O$ then

$$n = q + 1 + 2\sqrt{q} - z \tag{3}$$

is the potential order of the point P.

To find z the Rho Pollard method (Blake, 2000) can be used. It is a random method for computing collisions of elements of a finite group. The collision is found after approximately $\sqrt{q\pi/2}$ iterations. If the collision occurs the last thing to check is if n is prime and if it belongs to the Hasse range. If this is the case, then we have the base point and its order, else we repeat the procedure for new curve parameters (a and b), value q and thus the prime field can also be changed. For primality testing of small integers (< 341550071728321) a deterministic variant of Miller-Rabin Primality Test can be used (Jaeschke, 1993).

For efficient generation of SEC on the nodes we plan to investigate the possibilities to influence the curve parameters for which we want to find the curve order and investigate the methods to generate chains of SEC parameters.

2.4 Modified Cryptographic Protocols

Modified El'Gamal Encryption. To carry out encryption and decryption of messages using SEC some changes in the algorithms have to be made. The basis of encryption scheme is the El'Gamal scheme (Blake, 2000) with one small difference in the first step.

To encrypt a message $m \in (0, p)$ for a recipient a party does the following steps:

- Obtain the recipient's public key Q_R.
- Select a random or pseudo random integer number $k \in [1, p-1]$.
- Calculate an EC point $R = kP + T$, where T is a point on the curve, known for both parties and determined while curve parameters are established. T should be changed after each transaction between the sender and recipient of the message.
- Transform the message m into a point M lying on E, e.g. as described in (Washington, 2003).
- Calculate an EC point $S = kQ_R + M$.
- The message m is encrypted as the pair of EC points (R, S). These points are compressed before sending, thus only the x-coordinates are transmitted.

The recipient does the following to decrypt the message:

$$M = S - d_R R + d_R T \tag{4}$$

Where d_R is the private key of the message recipient.

Modified Digital Signature Scheme. Standard digital signature schemes (Koblitz, 1998) use the standard cryptographic hash functions for signing the messages. These hash functions produce outputs of 160 or even 512 bit length (NIST, 2010), thus they are not applicable in our digital signature protocol. In the case of SEC another solution has to be used. Current version supports only a signature scheme with message recovery. The signatures are generated for a specified recipient only. To sign the message the signer, which key pair is (k_S, Q_S), does the following steps:

- Convert message m into the point $M = (x_M, y_M)$ on the elliptic curve (in the same way as in modified encryption scheme)
- Compute
$$s = k^{-1}(x_M + y_M k_S), \text{ where } k \text{ is random} \tag{5}$$
- Encrypt M using the same k and the public key of the recipient. R and S are the encrypted message
- The signature is a triple (R, S, s)

Verification phase:

- Decrypt R and S to obtain the coordinates of M needed in the next steps of verification.
- Compute two values u_1, u_2:
$$u_1 = s^{-1} x_M, \qquad u_2 = s^{-1} y_M \tag{6}$$
- Verify the signature by checking if:
$$R = u_1 P + u_2 Q_S + T \tag{7}$$

3 SECURITY ANALYSIS

In this section we discuss three aspects of the security in our approach. The first considers the search area of an attacker not knowing the SEC in use. Let us consider a SEC based on a 32-bit finite field. Having an eavesdropped coordinate of some point on the elliptic curve an adversary has to decompress it to get the second coordinate. For decompression the knowledge about SEC parameters is needed. Without the knowledge about the second coordinate solving of the elliptic curve equation and finding its parameters is impossible. Finding the curve parameters on the basis of the eavesdropped x-coordinate of some point an adversary has to do the following:

1. Choose the order of the prime field, i.e. the prime integer q. She has to look in a set of
$$\frac{2^{32}}{\ln 2^{32}} \approx 193641447 \tag{8}$$
elements, because there are that many prime numbers of maximum 32-bit length.

2. Then for the prime field the adversary has to find the proper elliptic curve. There are (q^2-q) possible elliptic curves for prime field $\mathbb{F}_q$.
3. Now she can check if there exists a point with the eavesdropped x-coordinate on this elliptic curve. In the worst case each elliptic curve can have a point with this x-coordinate. So this information does not reduce the set of curves being suspected to be the right one. In the best case there is only one elliptic curve which contains a point with x-coordinate.
4. If there is a point with x-coordinate she can move to the next step, else she has to generate another elliptic curve, going back either to step 1 or 2.
5. In a standard cryptographic systems the base point is known. In our system it's kept secret. For each $E(\mathbb{F}_q)$ the average number of points on this curve is equal to $(q+1)$. Thus the probability of choosing the proper base point is

$$\left(\frac{1}{q+1}\right) \tag{9}$$

Let W denote the number of all elliptic curves over all considered prime fields. W is approximately equal to:

$$\sum_{n=0}^{m}(q_n^2-q_n), \quad \text{where} \quad m=\frac{2^{32}}{\ln 2^{32}} \tag{10}$$

So the probability that an adversary finds the right curve parameters is:

$$\left(\frac{1}{W}\right)\left(\frac{1}{q+1}\right) \tag{11}$$

The second security aspect is the ambiguity of the results even if the SEC parameters are known. Let us assume that the adversary receives a x-coordinate x_Q of a point Q lying on some SEC. She knows only that it is the multiple of the base point since all other information is kept secret. Let us assume that she has a set of curves that contain points with x_Q and this set includes the curve E. If $E(\mathbb{F}_q)$ has a prime order p and $Q=kP_i$, where $k\in\mathbb{F}_q$, $P_i\in E$ and $i\in[1,p-1]$, then the group of points on E looks as follows:

$$E=\{O,P_1,P_2,\ldots,P_{p-1}\}. \tag{12}$$

We already know that a group of points is cyclic and it has a prime order. There are no subgroups of E and there are no points $(\neq O)$ with order different from p. Thus, any point in this group can be a generator of E. So for $i=1,\ldots,(p-1)$ we have $(p-1)$ possible permutations:

$$E=\{O,P_i,2P_i,\ldots,(p-1)P_i\} \tag{13}$$

Where $<P_1>=\cdots=<P_{(p-1)}>$ and

$$\forall_{i,j,k\in[1,p-1]}\ iP_j\neq iP_k. \tag{14}$$

We can see that

$$\forall_{i\in[1,p-1]}\exists_{k\in[1,p-1]}\ kP_i=Q. \tag{15}$$

The third aspect relates to modified ElGamal encryption. As already mentioned the point T should be changed after each transaction between the sender and receiver. For example, at the beginning both parties agree on a start point T. This point is used in first transaction and after that the next one is computed. Both have to keep the number of the transaction and the previous point to compute the next one. It can be done as follows:

$$T_i=iT_{i-1}, \quad \text{where} \tag{16}$$

i is the number of the current transaction. When T would not be changed it could be possible to obtain the secret key of the receiver. Two different encryptions of the same message look as follows:

$$R_1=k_1P+T, \qquad S_1=M+k_1Q_R \tag{17}$$

$$R_2=k_2P+T, \qquad S_2=M+k_2Q_R \tag{18}$$

Having these one can compute:

$$R_1-R_2=k_1P+T-k_2P-T \tag{19}$$

$$R_1-R_2=(k_1-k_2)P \tag{20}$$

$$S_1-S_2=M+k_1Q_R-M-k_2Q_R=(k_1-k_2)Q_R \tag{21}$$

And since $Q_R=d_RP$:

$$S_1-S_2=(k_1-k_2)d_RP \tag{22}$$

finally:

$$(R_1-R_2)d_R=S_1-S_2 \tag{23}$$

Having some curves being suspected the adversary can decompress the points, compute the point subtraction using these and then solve the discrete logarithm problem to obtain the possible values of d_R for the suspected curves. Changing the value of T each time makes an attempt of finding d_R more complicated, because

$$(R_1-R_2)=(k_1-k_2)P+T_1-T_2 \tag{24}$$

$$(R_1-R_2)d_R\neq S_1-S_2 \tag{25}$$

For each curve on which point R exists and for each point suspected as a base point P the adversary has to find an integer k and point T for which $R=kP+T$. Because $k\in[1,p-1]$ and order of T is p she has to check $(p-1)p$ combinations. Looking for secret key for each point gives $(p-1)p^2$ combinations to check. If there are t curves, each of order p, the number of combinations is equal to $(p-1)p^2t$.

4 CONCLUSIONS AND FUTURE WORK

In this paper we presented a new security approach for WSN. We designed and proved new encryption and digital signature algorithms and a simple method for SEC generation.

The work on this approach is in its initial phase. Up to now we focused on theoretical solutions, proofs of correctness of modified algorithms. The next step will be an implementation of SEC cryptosystem on sensor nodes and investigate its costs, both computational and management overhead. We will study the ability of an attacker for finding SEC parameters on the basis of x-coordinate what will help us to estimate the lifetime of complete SEC cryptosystem. Then the methods for changing the SEC will be chosen and investigated. Depending on the lifetime it will be either generation of chains of SEC parameters or a fixed set with a method for picking up the right one. The necessity of using a trusted authority will also be verified. We also plan to check if the SEC cryptosystem is transferable to projective coordinates. It could be interesting due to the less computational effort when using projective coordinates (Blake, 2000). We also foresee an extension of the signature algorithm to support a signature that can be verified by any member of the group and to support an arbitrary size of the message. As already mentioned the presented Short Elliptic Curves are a hybrid symmetric/asymmetric Cryptography approach. In our next research steps we want to find an answer to the question where between these two kinds of cryptography our approach can be placed.

REFERENCES

Texas Instruments Inc. (2008). CC2420 datasheet 2.4 Ghz IEEE 802.15.4/zigbee RF transceiver. http://focus.ti.com/lit/ds/symlink/cc2420.pdf.

Freie Universitaet Berlin and FeuerWhere Project Partners, (2008). FeuerWhere Project official website. http://www.feuerwhere.de/.

Texas Instruments Inc. (2009). MSP430f15x, MSP430f16x, MSP430f161x Mixed Signal Microcontroller. http://focus.ti.com/lit/ds/symlink/msp430f1611.pdf.

NIST National Institute of Standards and Technology, (2010). http://www.nist.gov/index.html.

Moteiv Corp, (2006). Tmote Sky Low Power Wireless Sensor Module. http://sentilla.com/files/pdf/eol/tmote-sky-datasheet.pdf.

SIC Stiftung Secure Information and Communication Technologies, (2009). Crypto Software for Microcontrollers. http://jce.iaik.tugraz.at/sic/Products/Crypto-Software-for-Microcontrollers/Texas-Instruments-MSP430-Microcontrollers.

Blake, I., Seroussi, G. and Smart, N. (2000). *Elliptic Curves Cryptography*. Cambridge University Press, 1st edition.

Jaeschke, G. (1993). On strong pseudoprimes to several bases. *Mathematics of Computation*, 61:915–926.

Piotrowski, K., Langendoerfer, P. and Peter, S. (2006). How public key cryptography influences wireless sensor node lifetime. *SASN*.

Koblitz, N. (1998). *Algebraic Aspects of Cryptography*. Springer-Verlag, Berlin Heidelberg, 1st edition.

Washington, L. C. (2003). *Elliptic Curves Number Theory and Cryptography*. Chapman & Hall/CRC.