Kleptographic Attacks on Elliptic Curve Cryptosystems

Elsayed Mohamed and Hassan Elkamchouchi
Alexandria University, Alexandria, Egypt

Summary
This paper presents an approach to mount secretly embedded trapdoor with universal protection (SETUP) attacks on elliptic curve cryptosystems. The attacked cryptosystem used is the elliptic curve analog of ElGamal encryption. The attacker can obtain the user's confidential message covertly. The cryptographic black-box devices with this hidden trapdoor behave exactly like an honest devices while actually leaking the confidential message to the attacker only.

Key words:
Elliptic Curve Cryptography, Kleptography, Subliminal Channel, SETUP

1. Introduction

- **Elliptic Curves**

Elliptic curves are known for their security. The common fields used for encryption are prime fields and characteristic 2 fields. Elliptic curves over prime fields are on the form:
$E: y^2 = x^3 + ax + b \bmod p$
where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \bmod p$

The addition of two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ is calculated by:
$R(x_3, y_3) = P + Q$ where:
$x_3 = \lambda^2 - x_1 - x_2$,
$y_3 = \lambda(x_1 - x_3) - y_1$,
$\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P \neq Q$
$\lambda = (3x_1^2 + a)/2y_1$ if $P = Q$

The multiplication of points by a scalar is a series of doublings and additions of points. The multiplication by -1 converts P to $-P$ by negating the y coordinate of P, i.e., the negative of $P = (x, y)$ gives $-P = (x, -y)$. Similar formulas exist for elliptic curves over characteristic 2 fields.

- **Elliptic Curve Discrete Logarithm Problem (ECDLP)**

Given a point P of order n in an elliptic curve E over a finite field F_p and a point Q in E , the ECDLP is to find an integer m, where $0 \leq m \leq n - 1$, and $Q = m \times P$ if such a number exists.

- **Elliptic Curve Diffie-Hellman Problem (ECDHP)**

Given a point P of order n in an elliptic curve E over a finite field F_p and two points kP and lP where $0 \leq k, l \leq n - 1$, the ECDHP is to find the point ($k \times l \times P$). This problem is used in the elliptic curve Diffie-Hellman key exchange algorithm.

- **ElGamal Elliptic Curve Encryption Scheme (ElGamal-ECES)**

In the elliptic curve analog of ElGamal encryption a plaintext message represented as point M on an elliptic curve E is encrypted to the ciphertext C. H is a cryptographically secure hash function that generates values less than n. The system parameters are the elliptic curve E, the base point G of order n, the private key d and the public key $Q = dG$.

Encryption Algorithm:
Input: Plaintext message point M
Output: Ciphertext C
Choose a random integer $k \leq n - 1$
$A = kG$
$B = kQ + M$
$C = (A, B)$

Decryption Algorithm:
Input: Ciphertext $C = (A, B)$
Output: Plaintext message point M
$dA = d.kG = kQ$
$M = B - dA$

- **Subliminal Channels**

Subliminal channels can be used to convey information in the output of a cryptosystem in a way different from the intended output. This notion was put forth by Simmons [1]. He demonstrated how a prisoner could leak secret messages to an outside partner without the warden knowing what is going on. The warden has the ability to read every message but still cannot read the secret message embedded within the cover message. Simmons further developed the concept to other applications including DSA [2].

- **Kleptography**

Kleptography is defined as the study of stealing information securely and subliminally within the context of cryptographic systems [3]. A kleptographic attack on the discrete logarithm problem has been introduced by Young

and Yung in [3]. They defined a Secretly Embedded Trapdoor with Universal Protection (SETUP) as an algorithm that can be embedded within a cryptosystem to leak encrypted secret key information to the attacker in the output of that cryptosystem [4]. The encrypted secret key information is noticeable only to the attacker. The types of SETUP [3] and their definitions are listed below.

Definition 1. Assume that C is a black-box cryptosystem with a publicly known specification. A (regular) SETUP mechanism is an algorithmic modification made to C to get C' such that:

1. The input of $C`$ agrees with the public specifications of the input of C.
2. $C`$ computes efficiently using the attacker's public encryption function $E$ (and possibly other functions as well), contained within $C`$.
3. The attacker's private decryption function D is not contained within $C`$ and is known only by the attacker.
4. The output of $C`$ agrees with the public specifications of the output of C. At the same time, it contains published bits (of the user's secret key) which are easily derivable by the attacker (the output can be generated during key-generation or during system operation like message sending).
5. Furthermore, the output of C and C' are polynomially indistinguishable (as in [5]) to everyone except the attacker.
6. After the discovery of the specifics of the SETUP algorithm and after discovering its presence in the implementation (e.g. reverse-engineering of hardware tamper-proof device), users (except the attacker) cannot determine past (or future) keys.

Definition 2. A weak SETUP is a regular SETUP except that the output of C and C ' are polynomially indistinguishable to everyone except the attacker and the owner/user of the device who is in control (knowledge) of his or her own private key (i.e., requirement 5 above is changed).

Definition 3. A strong SETUP is a regular SETUP, but in addition we assume that the users are able to hold and fully reverse-engineer the device after its past usage and before its future usage. They are able to analyze the actual implementation of C' and deploy the device. However, the users still cannot steal previously generated/future generated keys, and if the SETUP is not always applied to future keys, then SETUP-free keys and SETUP keys remain polynomially indistinguishable.

Definition 4. A kleptogram is an encryption of a value (hidden value) that is displayed within the bits of an encryption/signature of a plaintext value (outer value). Note that we say that a kleptogram is an encryption of a value, not a plaintext message. It is often the case in kleptography that the device is not free to choose this value. The device may calculate this hidden value, and then use it (for the 'randomness') in a subsequent computation, thus compromising that computation.

Definition 5. A SETUP that has (m, n)-leakage bandwidth leaks m secret messages over the course of n messages that are output by the cryptographic device (or n of its executions).

2. Proposed ElGamal-ECES SETUP Attack

ElGamal-ECES is chosen to demonstrate the possibility of embedding SETUP attacks on elliptic curve encryption. Attacks similar to the one presented here are possible on other elliptic curve cryptosystems. The private key of the attacker is v and the public key is $V = vG$. Hashing an elliptic curve point can be defined as hashing its x coordinate. The device operates as follows:

Encryption Algorithm with SETUP:
Input: Plaintext message point M
Output: Ciphertext C

For the first time the algorithm runs:
Choose a random integer $k_1 \leq n-1$
$A_1 = k_1G$
$B_1 = k_1Q + M_1$
$C_1 = (A_1, B_1)$
Store k_1 in non-volatile memory

For the next run times:
$Z = a.k_1G + b.k_1V + h.jG + e.uV$, where:
a, b, h, e are fixed integers $< n$
$j, u \in_R \{0, 1\}$ are uniformly and independently chosen at random
$k_2 = H(Z)$
$A_2 = k_2G$
$B_2 = k_2Q + M_2$
$C_2 = (A_2, B_2)$
Store k_2 in non-volatile memory

The normal user is able to decrypt and retrieve the message M in a normal way at all times using his private key d. The attacker can retrieve M_2 and the next messages by obtaining C_1 and C_2 from the channel and computing k_2 as follows.

SETUP Decryption Algorithm:
Input: Ciphertext $C_1 = (A_1, B_1)$, $C_2 = (A_2, B_2)$
Output: Plaintext M_2
$Z_1 = aA_1 + b.vA_1 = a.k_1G + b.v.k_1G = a.k_1G + b.k_1V$
For each possible value of j, u:
{
$Z_2 = Z_1 + h.jG + e.uV$
$k_2 = H(Z_2)$
If $k_2G = A_2$ then the current k_2 is the right one so exit the loop
}

$M_2 = B_2 - k_2Q$

Thus M_2 is obtained without knowing the user's private key d.

3. Discussion and Analysis

A. Security

Since k_1 is random it follows that Z is uniformly distributed within the group generated by G. This SETUP attack is secure in the sense that a user not knowing the random choice k_1 cannot calculate the second private key k_2 as long as ECDHP is hard. This can be proven by supposing that an oracle A can solve the ECDH problem so that $A(aG, bG) = abG$. If A is applied on A_1 and V then: $A(A_1, bV) = b.v.k_1G = b.k_1V$, which can be used to calculate Z. Also an adversary that does not know the attacker's private key v cannot calculate Z and therefore cannot calculate k_2. This makes the universal protection property of the SETUP attack. Assuming that H is a pseudorandom function and that the device can be reverse-engineered, the outputs of C and C` are polynomially indistinguishable. This results from Z being uniformly distributed and H being a pseudorandom function. Even if the user knows his private key d he still cannot recover k. Thus the ElGamal-ECES SETUP attack is a strong SETUP as long as ECDHP is hard and the random parameter generated by the device is inaccessible to the user. The random values j and u are used to add randomization to further insure undetectability of SETUP in a black-box implementation. Adding them serves as a precaution so that if the random parameter k_i is available to the user and the hash function H is invertible, the user still cannot detect the presence of a SETUP in the device by running the device many times and guessing several different values of V. It also helps to curb trying to notice any possible probabilistic relations between some properties in V and some corresponding properties in Z. This kind of probabilistic detection by the user is very difficult in elliptic curve cryptosystems compared to discrete log systems where quadratic residuosity can be used to test a possible relation between the attacker's public key and Z [3]. This makes elliptic curve devices a better candidate for kleptographic attacks in addition to the improved security and key length advantages of elliptic curve systems.

B. Bandwidth

Retrieving one message requires the system to run twice. This leads to a bandwidth of (1, 2). By chaining the generation of k we can increase the bandwidth to (m, m + 1).

C. Implications for Hybrid Encryption

In hybrid encryption messages are encrypted by a symmetric cipher using a session key that is encrypted by public key encryption. In his case the message M_2 that the attacker has been able to decrypt by the attack above is actually a session key. Obtaining it enables the attacker to decrypt all messages encrypted with that session key.

4. Conclusion

We have shown that a strong SETUP attack can be mounted on ElGamal elliptic curve encryption. This enables a malicious manufacturer of black-box cryptosystems like smart card devices to implement such attacks and thus have the exclusive ability to decrypt the user's encrypted messages. The output of a dishonest device is indistinguishable from the output of an honest one.

References

[1] G. J. Simmons, "The Prisoner's Problem and the Subliminal Channel", *Crypto '83*, pp. 51-67, 1983.

[2] G. J. Simmons, "Subliminal Communication is Easy Using the DSA", *Eurocrypt '93*, pp. 218-232, 1993.

[3] A. Young, M. Yung, "Kleptography: Using Cryptography Against Cryptography", *Eurocrypt '97*, pp. 62-74.

[4] A. Young, M. Yung, "The Dark Side of Black-Box Cryptography or Should We Trust Capstone?", *Crypto '96*, pp. 89-103.

[5] S. Goldwasser, S. Micali, "Probabilistic Encryption", *J. Comp. Sys. Sci.* 28, pp. 270-299, 1984.