ECIES

NES/DOC/RHU/WP3/007/c

Rachel Shipsey
Royal Holloway, University of London

March 1, 2001

1 Algorithm Summary

The Elliptic Curve Integrated Encryption Scheme (ECIES) is a public key encryption scheme submitted by Certicom. ECIES is designed to be semantically secure in the presence of an active adversary capable of launching chosen plaintext and chosen ciphertext attacks.

1.1 Elliptic Curve Parameters

The elliptic curve parameters required are either \(T = (p,a,b,G,n,h)\) where

- \(p\) is a prime and \(a,b\) are elements of \(\mathbb{F}_p\) with \(4a^3 + 27b^2 \neq 0 \mod p\) defining the elliptic curve
  \[
  E : y^2 = x^3 + ax + b \mod p
  \]
  Care is taken to ensure that \(\#E(\mathbb{F}_p) \neq p\) and that \(p^B \neq 1 \mod n\) for \(1 \leq B \leq 20\) and therefore \(E\) is not a weak elliptic curve for cryptographic purposes.
- \(G\) is a base point on \(E(\mathbb{F}_p)\) with prime order \(n\)
- \(h\) is the cofactor \(h = \#E(\mathbb{F}_p)/n\) with \(h \leq 4\)

or \(T = (m,f(x),a,b,G,n,h)\) where

- \(m\) is an integer specifying the finite field \(\mathbb{F}_{2^m}\)
- \(f(x)\) is an irreducible binary polynomial of degree \(m\) specifying the representation of \(\mathbb{F}_{2^m}\)
\begin{itemize}
  \item $a, b$ are elements of $\mathbb{F}_{2^m}$ specifying the elliptic curve
  \[ E : y^2 + xy = x^3 + ax^2 + b \text{ in } \mathbb{F}_{2^m} \]
  Again care is taken to avoid cryptographically weak curves by ensuring that $m$ is prime, $b \neq 0$, $\#E(\mathbb{F}_{2^m}) \neq 2^m$ and $2^nB \neq 1 \mod n$ for $1 \leq B \leq 20$.
  \item $G, n, h$ are the base point, order and cofactor as above
\end{itemize}

In order to use ECIES, the sender and the recipient must agree upon:

\begin{itemize}
  \item a MAC scheme denoted by $MAC$ which produces tags of length $maclen$;
  \item a symmetric encryption scheme denoted by $ENC$, taking keys of length $keylen$;
  \item a key derivation function denoted by $KDF$ producing keys of length $keylen + maclen$;
  \item elliptic curve domain parameters $T = (p, a, b, G, n, h)$ or $T = (m, f(x), a, b, G, n, h)$ as described above.
\end{itemize}

### 1.1.1 Public and Private Keys

The recipient selects a random integer, $d$, in the interval $[1, n - 1]$ and computes $Q = dG$. The private key of the recipient is $d$ and the public key is $Q$.

The submission includes a table giving a range of public key sizes (from 112 to 512 bits) which may be used as appropriate depending on the security level required of the system.

### 1.2 The Encryption Operation

In order to encrypt a message $M$ using ECIES with the public key $Q$, the sender takes the following steps:

\begin{enumerate}
  \item Select a (temporary) random integer $k$ in the interval $[1, n - 1]$ and compute $R = kG = (x_R, y_R)$.
  \item Convert the point $R$ into an octet string $\hat{R}$.
  \item Use the Diffie-Hellman primitive to obtain a shared secret field element $z \in \mathbb{F}_q$ from the temporary secret key $k$ and the public key $Q$ (e.g. Compute point $P = (x_P, y_P) = kQ$ and let $z = x_P$).
  \item Convert $z$ into an octet string $Z$.
\end{enumerate}
5. Use the KDF to generate keying data $K$ from $Z$ and [sharedinfo1].

6. Parse the leftmost $keylen$ octets of $K$ as an encryption key $EK$ and the rightmost $maclen$ octets of $K$ as a MAC key $MK$.

7. Use the symmetric encryption scheme with key $EK$ to encrypt message $M$ into ciphertext $EM$.

8. Use the MAC scheme with key $MK$ to produce a tag $D$ for $EM \ || \ [sharedinfo2]$.\(^1\)

9. Output $C = \hat{R} \ || \ EM \ || \ D$.

1.3 The Decryption Operation

Given the ciphertext $C = \hat{R} \ || \ EM \ || \ D$, together with private key $d$, the recipient decrypts $C$ to recover message $M$ as follows:

1. Convert the octet string $\hat{R}$ into an elliptic curve point $R = (x_R, y_R)$.

2. Use the Diffie-Hellman primitive to compute the shared key $z$. (For example, if $P = (x_P, y_P) = kQ$ and $z = x_P$ as described above, then compute $dR = dkG = kQ = P = (x_P, y_P)$ and set $z = x_P$).

3. Convert $z$ into an octet string $Z$.

4. Use the KDF to generate keying data $K$ from $Z$ and [sharedinfo1].

5. Parse the leftmost $keylen$ octets of $K$ as an encryption key $EK$ and the rightmost $maclen$ octets of $K$ as a MAC key $MK$.

6. Use the tag checking operation of the MAC scheme to check that $D$ is the tag on $EM \ || \ [sharedinfo2]$ under MAC key $MK$.

7. Use the symmetric decryption scheme to decrypt $EM$ using key $EK$ and thus recover message $M$.

2 ECIES: Security Assumptions

The security of ECIES relies on

- The difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Elliptic Curve Diffie-Hellman Problem (ECDHP),

\(^1\)The parameters [sharedinfo1] and [sharedinfo2] are octet strings which consist of some data common to the sender and the recipient. The inclusion of the parameters [sharedinfo1] and [sharedinfo2] is optional.
• The use of secure random or pseudorandom number generators for key generation,
• The resistance to attacks on the symmetric encryption scheme used (3-key TDES or XOR),
• The resistance to attacks on the MAC scheme,
• The resistance to attacks on the key derivation function,
• The security of the primitives for key validation.

2.1 ECDLP

The ECDLP is the problem of solving $Q = dG$, given $Q$ and $G$. The usual methods to approach this problem are:

• Exhaustive search,
• The Baby step-giant step method,
• Pollard’s $\rho$ method,
• The Pohlig-Hellman algorithm,

In particular cases, such as supersingular curves and abnormal curves there exist special algorithms to solve the ECDLP; such curves can be avoided by a suitable choice of the coefficients of the curve.

2.2 Recovering Message $M$

Message $M$ is encrypted using symmetric encryption algorithm $ENC$ with key $EK$. If the encryption algorithm is weak, then we may be able to recover $M$ without knowledge of the key $EK$. It is assumed that a suitably secure symmetric encryption algorithm is chosen so that such an attack is not possible. The symmetric encryption schemes recommended for use in the submission are: 3-key TDES in CBC mode; XOR encryption scheme; and (when it has passed through the standardisation process) the AES scheme Rijndael.

Alternatively, it may be possible to find the value of the temporary secret value $k$, and thus compute elliptic curve point $kP$ and so find $z, K, EK$ and $MK$. We can then recover the message $M$ which was encrypted using key $EK$. Since a different value of $k$ is used for each message, this attack will only recover the particular message $M$ and does not leak any information about the secret key $d$. 

4
2.3 A Possible Security Issue

As pointed out by Abdalla, Bellare and Rogaway in their paper *DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem*, there may be a problem with step 3 of the encryption operation if the secret element $z$ is obtained by multiplying the public key $Q$ by the temporary secret key $k$ so that $z = x_kQ$. The problem is that there may exist an element $k'$ such that $x_{k'}Q = z$ but $k' \neq k$. This could lead to the scheme being insecure in the malleable sense which in turn implies that the scheme is insecure against adaptive chosen ciphertext attack, since otherwise it would be non-malleable.

To illustrate this consider the ciphertexts $C_1 = (R_1 || EM || D)$ and $C_2 = (R_2 || EM || D)$. If, for example, $P_1 = k_1Q$ and $P_2 = -k_1Q$ then $z_1 = z_2$ and the two ciphertexts $C_1$ and $C_2$ decrypt to give the same message $M$. This is what is meant by saying that the scheme may be insecure in the malleable sense.

The DHAES paper uses both the temporary private key $k$ as well as the temporary public key $kP$ and the scheme public key $Q$ in order to compute $z$ and ensure that the scheme is non-malleable. A similar approach may be taken to ensure that ECIES is also non-malleable.

3 Conclusion

Provided that ECIES is used as designed it appears to be as secure as claimed by the submitters. That is, if the pseudo-random number generator and MAC function used in the scheme remain unbroken, and if the ECDLP is intractable, then ECIES is semantically secure in the presence of an active adversary. Certain attacks may be used if, for example, the elliptic curve used is weak, but the submission lists these attacks and the countermeasures taken when choosing the scheme parameters in order to negate any such weaknesses.