

Development of ID-Based Encryption

Authors: *Katsuyuki Takashima** and *Tsutomu Sakagami**

1. Introduction

The recent development of ID-based encryption is attracting attention because it enables the use of ID information as a public key. After the concept of ID-based encryption was first proposed by Shamir in 1984⁽¹⁾, many years passed before a working system was implemented by Sakai and Kasahara using their ID-based key sharing scheme in 1999⁽²⁾ and Boneh et al. in 2001⁽³⁾ using their ID-based encryption algorithm with proven security. In ID-based encryption, an important role is played by pairing operation on elliptic curves. In this paper, Section 2 provides a technical overview of ID-based encryption; Section 3 introduces our efficient pairing operation method; and Section 4 discusses an experimental encrypted mail system.

2. ID-Based Encryption

Each ID-based encryption system needs an ID-based private key generator (PKG), which generates a private key for an arbitrary ID. It consists of four functions: "parameter generation function" and "private key generation function" utilized by the PKG, and "encryption function" and "decryption function" utilized by the users.

- The parameter generation function uses the bit length of the key as input data to generate system parameters for use throughout the system and a PKG private key.
- The private key generation function generates a user private key from ID information provided using the system parameters and the PKG private key.
- The encryption function generates ciphertext from plaintext using the system parameters and the ID.
- The decryption function generates plaintext from ciphertext using the system parameters and the user private key.

Note that the ID, an input to the encryption function, is the public key. In an ordinary public key encryption scheme, a public key certificate, which is the signature to the public key, is used to ensure the validity of the public key for the encryption. In ID-based encryption, however, a public key certificate is not required because any ID can be made into a public key, which increases the convenience of this method.

For ID-based encryption to work properly, the abovementioned four functions must satisfy the following two conditions:

1. Properly ciphertext can be decrypted to the original plaintext.
2. Any private key corresponding to any ID other than ID_1 cannot retrieve any information about plaintext corresponding to ciphertext addressed to ID_1 .

The second condition is the security requirement against collusion attacks.

3. Improved Algorithm for Pairing operation on Elliptic Curves

While various schemes have been proposed to realize an ID-based encryption system as described in Section 2, all of the practical schemes are based on pairing operation on elliptic curves.

An elliptic curve E is defined by $Y^2 = X^3 + aX + b$ (where a and b are elements in a finite field). For points P and Q on the curve, algebraic addition $P + Q$ is defined. Also, pairing operation on E is given as a bilinear map $\text{map}(P, Q) \rightarrow e(P, Q)$ where $e(P, Q)$ is in (an extension of) the finite field. In the following discussion, specific pairing called "Tate pairing e " is treated. One of the properties of pairing e is bilinearity, which is the most important characteristic for ID-based encryption and is expressed as:

$$e(uP, vQ) = e(P, Q)^{uv}$$

Due to this bilinearity, ID-based encryption and various other crypto applications can be used in practice.

Pairing operation largely consists of Miller's algorithm and final exponentiation. Extensive studies have been made to improve the efficiency of Miller's algorithm in relation to the selection of relevant parameters.

A commonly used Miller's algorithm is Algorithm 1. While a detailed explanation is not included here, computation according to Algorithm 1 is performed using lines l and v that appear in the addition and doubling algorithm on the elliptic curve.

Many reports have been published on the improved efficiency of the above algorithm. We have modified the method proposed by Scott⁽⁵⁾ so that the security can be flexibly adjusted, using a specific curve $Y^2 = X^3 + b$ where $p \equiv 1 \pmod{3}$ is the order of the finite field, which allows fast computation. This curve has the map $(x, y) \rightarrow (\beta x, y)$, where β is a primitive cubic root of 1. Using this map, faster computation can be achieved.

Algorithm 1 Miller's algorithm**Input:** Points P and Q on E .**Output:** Miller variable.

- 1: Select a point S on E .
- 2: $Q' \leftarrow Q + S, T \leftarrow P$.
- 3: $i \leftarrow \lfloor \log_2(r) \rfloor - 1, f \leftarrow 1$.
- 4: **while** $m \geq 0$ **do**
- 5: Calculate lines l and v for doubling T .
- 6: $T \leftarrow 2T$.
- 7: $f \leftarrow f^2 \frac{l(Q')v(S)}{v(Q')l(S)}$.
- 8: **If** the i -th bit of r is 1, **then**
- 9: Calculate lines l and v for adding T and P .
- 10: $T \leftarrow T + P$.
- 11: $f \leftarrow f \frac{l(Q')v(S)}{v(Q')l(S)}$
- 12: **end if**
- 13: $i \leftarrow i - 1$.
- 14: **end while**
- 15: Output f .

Fig. 1 Miller's algorithm

4. Prototype Encrypted Mail System

An experimental encrypted mail system was constructed applying the ID-based encryption scheme. We developed an ID-based private key generator (PKG) and encrypted mail client that is utilized by the users to transmit/receive encrypted mail. The experimental system makes it possible to transmit and receive encrypted mail without managing public key certificates or advance sharing of passwords. Implementation of this system is described in the following sections.

4.1 PKG

For ID-based encryption, the keystone of the system is PKG. It plays an essential role in the overall operation of the ID-based encryption system including distribution of the system parameters $pkey_{PKG}$ to users and generation of user private keys. In our experimental system, considering recent business network environments such as the use of firewalls and proxy servers, the http/https scheme is used as the protocol for encrypted mail clients to access the PKG. In addition, considering the need for complex data communication between the encrypted mail client and the PKG using http/https, SOAP is used as the protocol for inter-application communication. Since the http/https protocol is used as the low-level protocol, PKG is implemented as a servlet on the Web-based application server.

4.2 Encrypted mail client

Outlook 2003 is used as the encrypted mail client, because of its expandability with add-on features and our previous experience with feature expansion. Low-level library software is written in C/C++, and high-level GUI programs are in VB.

4.3 Data communication between PKG and mail client

The data format for communication between PKG and the mail client is defined using XML because SOAP over http/https is used as the low-level protocol.

4.4 Encrypted mail data

Encrypted mail transmitted from the encrypted mail client is formatted using Mitsubishi's proprietary capsular scheme. This capsular data format, which has long been studied at our laboratory, allows not only data encryption but the definition of usage restrictions on the received data (printable or not, copy/paste allowed or not, etc.).

4.5 Future prospects

Since ID-based encryption is a new encryption scheme, related standards are still under consideration by the IETF, including the method for distributing system parameters from PKG to the client, and how to transfer a private key from PKG to the client. The IETF is considering the Cryptographic Message Syntax (CMS) used in the Secure/Multipurpose Internet Mail Extension (S/MIME) with additional data format for ID-based encryption (see Reference (4)). Although our own scheme is used in the current implementation, we intend to develop a system that allows us to propose standardization to the IETF and that conforms to the standards.

5. Conclusion

Regarding ID-based encryption that uses ID information as the public key and allows easy introduction of public key encryption function, we proposed an improved algorithm and presented an experimental encrypted mail system.

References

- (1) A. Shamir, "Identity-based cryptosystems and signature schemes," *Crypto 84*, pp. 47-53, Springer Verlag, 1985.
- (2) K. Ohgishi, R. Sakai and M. Kasahara, "Basic consideration on ID key sharing scheme on elliptic curves," *IEICE Technical Report, ISEC99-57*, pp. 37-42, 1999.
- (3) D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *Crypto 2001*, pp. 213-229, Springer Verlag, 2001.

(4) IETF Internet Draft "Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the Cryptographic Message Syntax (CMS)."

(5) K. Takashima, "Scaling security of elliptic curves with fast pairing using efficient endomorphisms," IEICE Trans. on Fundamentals, Vol. E90-A, No. 1, pp. 152-159, Jan. 2007.

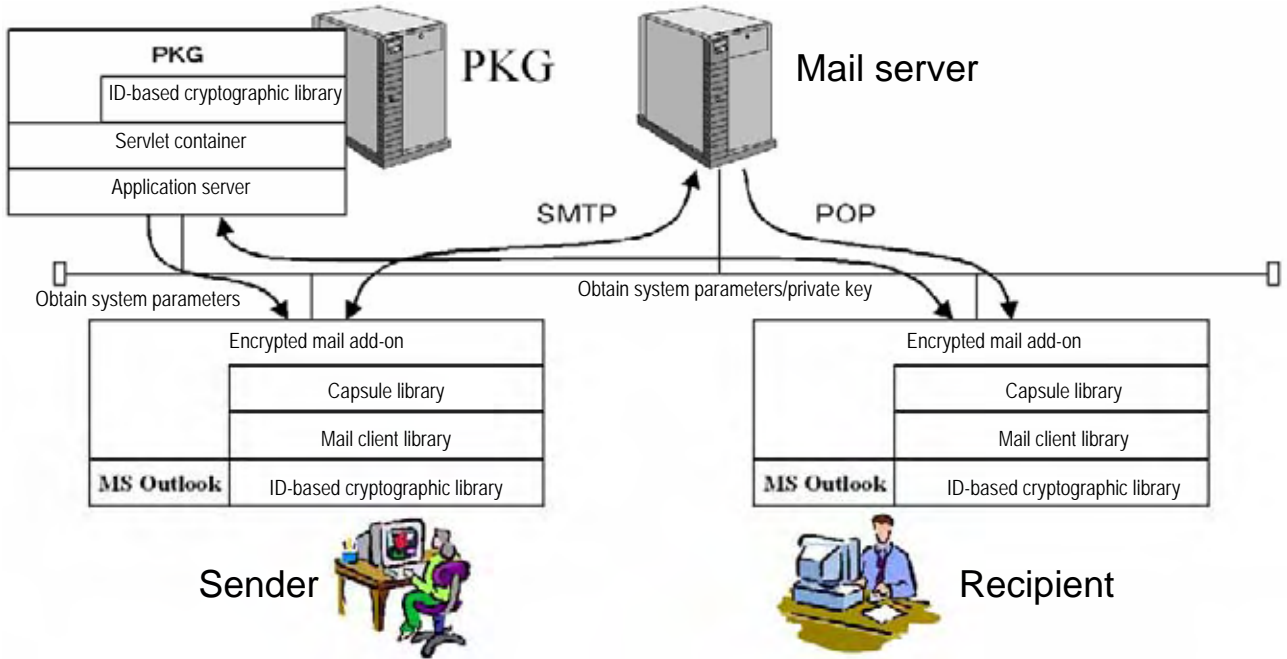


Fig. 2 Configuration of prototype ID-based encryption system