Sakai–Kasahara scheme

The **Sakai–Kasahara scheme**, also known as the Sakai–Kasahara key encryption algorithm (**SAKKE**), is an identity-based encryption (IBE) system proposed by Ryuichi Sakai and Masao Kasahara in 2003.[1] Alongside the Boneh–Franklin scheme, this is one of a small number of commercially implemented identity-based encryption schemes. It is an application of pairings over elliptic curves and finite fields. A security proof for the algorithm was produced in 2005 by Chen and Cheng.[2] SAKKE is described in Internet Engineering Task Force (IETF) RFC 6508.[3]

As a specific method for identity-based encryption, the primary use case is to allow anyone to encrypt a message to a user when the sender only knows the public identity (e.g. email address) of the user. In this way, this scheme removes the requirement for users to share public certificates for the purpose of encryption.

Contents

Description of scheme

The Sakai–Kasahara scheme allows the encryption of a message $\mathbb{M}$ to an receiver with a specific identity, I_U. Only the entity with the private key, K_U, associated to the identity, I_U, will be capable of decrypting the message.

As part of the scheme, both the sender and receiver must trust a Private Key Generator (PKG), also known as a Key Management Server (KMS). The purpose of the PKG is to create the receiver's private key, K_U, associated to the receiver's identity, I_U. The PKG must securely deliver the identity-specific private key to the receiver, and PKG-specific public parameter, Z, to all parties. These distribution processes are not considered as part of the definition of this cryptographic scheme.

Preliminaries

The scheme uses two multiplicative groups E and G. It is assumed:

- The Diffie-Hellman problem is hard in E. Meaning that given two members of the group P and Q, it is hard to find x such that $[x].P = Q$.
- The Diffie-Hellman problem is hard in G. Meaning that given two members of the group g and t, it is hard to find x such that $g^x = t$.

- There is a bilinear map, a Tate-Lichtenbaum pairing, $e(,)$ from E to G. This means that for P a member of E and for $g = e(P, P)$ a member of G:

$$e(P, [x].P) = e([x].P, P) = e(P, P)^x = g^x$$

Frequently, E is a supersingular elliptic curve, such as $E : y^2 = x^3 - 3x$ (over a finite field of prime order p). A generator P of prime order q is chosen in E. The group G is the image due to the pairing of the group generated by P (in the extension field of degree 2 of the finite field of order p).

Two hash functions are also required, H_1 and H_2. H_1 outputs a positive integer, x, such that $1 < x < q$. H_2 outputs n bits, where n is the length of the message $\mathbb{M}$.

Key generation

The PKG has a master secret z where $1 < z < q$, and a public key $Z = [z].P$ which is a point on E. The PKG generates the private key, K_U, for the user with identity ID_U as follows:

$$K_U = [\frac{1}{z+H_1(ID_U)}].P$$

Encryption

To encrypt a non-repeating message $\mathbb{M}$, the sender requires receiver's identity, ID_U and the public PGK value Z. The sender performs the following operation.

1. Create: $id = H_1(ID_U)$
2. The sender generates r using $r = H_1(\mathbb{M}||id)$
3. Generate the point R in E:

$$R = [r].([id].P + Z)$$

4. Create the masked message:

$$S = \mathbb{M} \oplus H_2(g^r)$$

5. The encrypted output is: (R, S)

Note that messages may not repeat, as a repeated message to the same identity results in a repeated ciphertext. There is an extension to the protocol should messages potentially repeat.

Decryption

To decrypt a message encrypted to ID_U, the receiver requires the private key, K_U from the PKG and the public value Z. The decryption procedure is as follows:

1. Compute $id = H_1(ID_U)$
2. Receive the encrypted message: (R, S).
3. Compute:

$$w = e(R, K_U)$$

4. Extract the message:

$$\mathbb{M} = S \oplus H_2(w)$$

5. To verify the message, compute $r = H_1(\mathbb{M}||id)$, and only accept the message if:

$$[r].([id].P + Z) \equiv R$$

Demonstration of algorithmic correctness

The following equations demonstrate the correctness of the algorithm:

$$w = e(R, K_U) = e([r].([id].P + Z), K_U) = e([r].([id].P + [z].P), K_U) = e([r(id + z)].P, K_U)$$

By the bilinear property of the map:

$$w = e([r(id + z)].P, K_U) = e([r(id + z)].P, [\frac{1}{(id+z)}].P) = e(P, P)^{\frac{r(id+z)}{(id+z)}} = g^r$$

As a result:

$$S \oplus H_2(w) = (\mathbb{M} \oplus H_2(g^r)) \oplus H_2(w) = \mathbb{M}$$

Standardisation

There are two standards relating to this protocol:

- Initial standardisation of scheme was begun by IEEE in 2006.[4]
- The scheme was standardised by the IETF in 2012 within RFC 6508. The scheme is used as part of the MIKEY-SAKKE protocol, defined in RFC 6509.

Cryptographic libraries and implementations

The scheme is part of the MIRACL cryptographic library.

See also

- ID-based encryption

References

1. Sakai, Ryuichi; Kasahara, Masao (2003). "ID Based cryptosystems with pairing on elliptic curve" (https://eprint.iacr.org/2003/054.pdf) (PDF). *Cryptography ePrint Archive*. 2003/054.
2. Chen, L.; Cheng, Z. "Security proof of Sakai-Kasahara's identity-based encryption scheme" (http://eprint.iacr.org/2005/226.pdf) (PDF). *Cryptography ePrint Archive*. 2005/226.
3. Groves, M. (February 2012). *Sakai-Kasahara Key Encryption (SAKKE)* (https://tools.ietf.org/html/rfc6508). IETF. doi:10.17487/RFC6508 (http://dx.doi.org/10.17487%2FRFC6508). RFC 6508. https://tools.ietf.org/html/rfc6508.
4. Barbosa, M. (June 2006). "SK-KEM: An Identity-Based KEM" (http://grouper.ieee.org/groups/1363/IBC/submissions/Barbosa-SK-KEM-2006-06.pdf) (PDF). IEEE. P1363.3.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Sakai–Kasahara_scheme&oldid=839421303"

This page was last edited on 3 May 2018, at 09:30 (UTC).