WIKIPEDIA

Cramer–Shoup cryptosystem

The **Cramer–Shoup system** is an asymmetric key encryption algorithm, and was the first efficient scheme proven to be secure against adaptive chosen ciphertext attack using standard cryptographic assumptions. Its security is based on the computational intractability (widely assumed, but not proved) of the decisional Diffie–Hellman assumption. Developed by Ronald Cramer and Victor Shoup in 1998, it is an extension of the ElGamal cryptosystem. In contrast to ElGamal, which is extremely malleable, Cramer–Shoup adds other elements to ensure non-malleability even against a resourceful attacker. This non-malleability is achieved through the use of a universal one-way hash function and additional computations, resulting in a ciphertext which is twice as large as in ElGamal.

Contents

Adaptive chosen ciphertext attacks

The definition of security achieved by Cramer–Shoup is formally termed "indistinguishability under adaptive chosen ciphertext attack" (IND-CCA2). This security definition is currently the strongest definition known for a public key cryptosystem: it assumes that the attacker has access to a decryption oracle which will decrypt any ciphertext using the scheme's secret decryption key. The "adaptive" component of the security definition means that the attacker has access to this decryption oracle both before and after he observes a specific target ciphertext to attack (though he is prohibited from using the oracle to simply decrypt this target ciphertext). The weaker notion of security against non-adaptive chosen ciphertext attacks (IND-CCA1) only allows the attacker to access the decryption oracle before observing the target ciphertext.

Though it was well known that many widely used cryptosystems were insecure against such an attacker, for many years system designers considered the attack to be impractical and of largely theoretical interest. This began to change during the late 1990s, particularly when Daniel Bleichenbacher demonstrated a practical adaptive chosen ciphertext attack against SSL servers using a form of RSA encryption.[1]

Cramer–Shoup was not the first encryption scheme to provide security against adaptive chosen ciphertext attack. Naor–Yung, Rackoff–Simon, and Dolev–Dwork–Naor proposed provably secure conversions from standard (IND-CPA) schemes into IND-CCA1 and IND-CCA2 schemes. These techniques are secure under a standard set of cryptographic assumptions (without random oracles), however they rely on complex zero-knowledge proof techniques, and are inefficient in terms of computational cost and ciphertext size. A variety of other approaches, including Bellare/Rogaway's OAEP and Fujisaki–Okamoto achieve efficient constructions using a mathematical abstraction known as a random oracle. Unfortunately, to implement these schemes in practice requires the substitution of some practical function (e.g., a cryptographic hash function) in place of the random oracle. A growing body of evidence suggests the insecurity of this approach,[2] although no practical attacks have been demonstrated against deployed schemes.

The cryptosystem

Cramer–Shoup consists of three algorithms: the key generator, the encryption algorithm, and the decryption algorithm.

Key generation

- Alice generates an efficient description of a cyclic group G of order q with two distinct, random generators g_1, g_2.
- Alice chooses five random values (x_1, x_2, y_1, y_2, z) from $\{0, \ldots, q-1\}$.
- Alice computes $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^z$.
- Alice publishes (c, d, h), along with the description of G, q, g_1, g_2, as her public key. Alice retains (x_1, x_2, y_1, y_2, z) as her secret key. The group can be shared between users of the system.

Encryption

To encrypt a message m to Alice under her public key $(G, q, g_1, g_2, c, d, h)$,

- Bob converts m into an element of G.
- Bob chooses a random k from $\{0, \ldots, q-1\}$, then calculates:
  - $u_1 = g_1^k, u_2 = g_2^k$
  - $e = h^k m$
  - $\alpha = H(u_1, u_2, e)$, where *H*() is a universal one-way hash function (or a collision-resistant cryptographic hash function, which is a stronger requirement).
  - $v = c^k d^{k\alpha}$
- Bob sends the ciphertext (u_1, u_2, e, v) to Alice.

Decryption

To decrypt a ciphertext (u_1, u_2, e, v) with Alice's secret key (x_1, x_2, y_1, y_2, z),

- Alice computes $\alpha = H(u_1, u_2, e)$ and verifies that $u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^\alpha = v$. If this test fails, further decryption is aborted and the output is rejected.
- Otherwise, Alice computes the plaintext as $m = e/(u_1^z)$.

The decryption stage correctly decrypts any properly-formed ciphertext, since

$$u_1^z = g_1^{kz} = h^k \text{, and } m = e/h^k.$$

If the space of possible messages is larger than the size of G, then Cramer–Shoup may be used in a hybrid cryptosystem to improve efficiency on long messages.

References

1. Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. Advances in Cryptology — CRYPTO '98. [1] (http://citeseer.ist.psu.edu/bleichenbacher98chosen.html)
2. Ran Canetti, Oded Goldreich, Shai Halevi. *The Random Oracle Methodology, Revisited* (http://doi.acm.org/10.1145/1008731.1008734). Journal of the ACM, 51:4, pages 557–594, 2004.

- Ronald Cramer and Victor Shoup. "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack." (https://link.springer.com/chapter/10.1007%2FBFb0055717) in proceedings of Crypto 1998, LNCS 1462, p. 13ff (ps (http://homepages.cwi.nl/~cramer/papers/cs.ps),pdf (http://knot.kaist.ac.kr/seminar/archive/46/46.pdf))

- Toy implementations of Cramer–Shoup in Emacs Lisp and Java (http://www.verify-it.de/sub/cramer_shoup.html)
- 1998 vintage news coverage of Cramer and Shoup's publication in Wired News (https://www.wired.com/news/technology/0,1282,14590,00.html) and in Bruce Schneier's Crypto-Gram (https://web.archive.org/web/20060426194426/http://packetstorm.linuxsecurity.com/mag/crypto-gram/crypto-gram-9809.html)
- Ronald Cramer and Victor Shoup: "Universal hash proofs and a paradigm for chosen ciphertext secure public key encryption." in proceedings of Eurocrypt 2002, LNCS 2332, pp. 45–64. Full Version (pdf) (http://www.shoup.net/papers/uhp.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cramer–Shoup_cryptosystem&oldid=797643848"

This page was last edited on 28 August 2017, at 11:40 (UTC).