The Cramer-Shoup Cryptosystem

Eileen Wagner

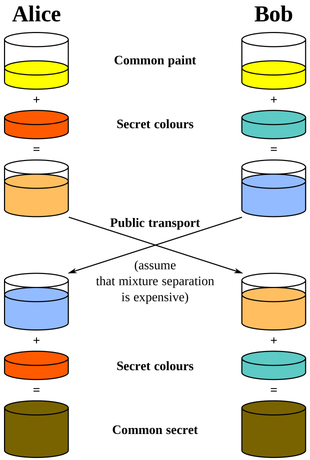
October 22, 2014

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. [2]

Outline

Outline

Public-key encryption



Diffie-Hellman
key exchange

`http://en.wikipedia.org/wiki/File:Diffie-Hellman_Key_Exchange.svg`

ElGamal encryption

Alice

Gen: $(q, g) \leftarrow \mathcal{G}(1^n)$

$G = \langle g \rangle$ a group, $|G| = q$

$sk = x \leftarrow \mathbb{Z}_q$

$h := g^x$

for $m \in G$: get $r \leftarrow \mathbb{Z}_q$

$\text{Enc}_{pk}(m) = (g^r, h^r m)$

$$\xrightarrow[(g^r,\, h^r m)]{pk = (g, q, h)}$$

Bob

$$\begin{aligned}\text{Dec}_{sk}(c_1, c_2) &= c_2 / c_1^x \\ &= h^r m / (g^r)^x \\ &= m\end{aligned}$$

Important results

How secure are our schemes?

Important results

How secure are our schemes?

- If the Decisional Diffie-Hellman problem is hard, then ElGamal is CPA-secure.
- If the RSA-assumption holds, then padded RSA is CCA-secure.

Important results

How secure are our schemes?

- If the Decisional Diffie-Hellman problem is hard, then ElGamal is CPA-secure.
- If the RSA-assumption holds, then padded RSA is CCA-secure.

Decisional Diffie-Hellman Problem

$$|\Pr[\mathcal{A}(G, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^{xy}) = 1]| \leq \mathrm{negl}(n)$$

CCA1 vs. CCA2

Malleability

An encryption algorithm is malleable if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext.

CCA1 vs. CCA2

Malleability

An encryption algorithm is malleable if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext.

For example, in ElGamal, given (c_1, c_2) an adversary can query $(c_1, t \cdot c_2)$, which is a valid decryption for tm.

CCA1 vs. CCA2

Adaptive chosen ciphertext attacks

An interactive chosen-ciphertext attack in which the adversary sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts.

CCA1 vs. CCA2

Adaptive chosen ciphertext attacks

An interactive chosen-ciphertext attack in which the adversary sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts.

$\rightarrow$ CCA2-security is equivalent to non-malleability [1]

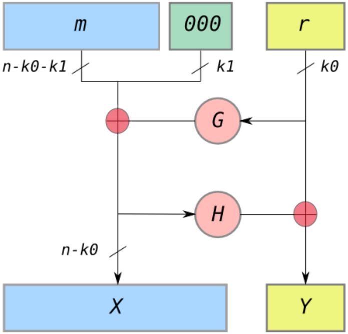
CCA1 vs. CCA2

Adaptive chosen ciphertext attacks

An interactive chosen-ciphertext attack in which the adversary sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts.

$\rightarrow$ CCA2-security is equivalent to non-malleability [1]
A CCA1-attack is also called a lunchtime attack.

Recall: OAEP for RSA



Optimal asymmetric encryption padding

http://en.wikipedia.org/wiki/File:Oaep-diagram-20080305.png

Outline

1. Motivation
   - What we've seen so far
   - Stronger notions of security
2. The Encryption Scheme
   - Cramer-Shoup
   - Proof of Security
   - Features
3. History & Implementation
   - People
   - Implementation
4. Conclusion

ElGamal encryption

Alice

Gen: $(q, g) \leftarrow \mathcal{G}(1^n)$

$G = \langle g \rangle$ a group, $|G| = q$

$sk = x \leftarrow \mathbb{Z}_q$

$h := g^x$

for $m \in G$: get $r \leftarrow \mathbb{Z}_q$

$\mathrm{Enc}_{pk}(m) = (g^r, h^r m)$

$$\xrightarrow[(g^r,\, h^r m)]{pk = (g, q, h)}$$

Bob

$$\begin{aligned} \mathrm{Dec}_{sk}(c_1, c_2) &= c_2 / c_1^x \\ &= h^r m / (g^r)^x \\ &= m \end{aligned}$$

Cramer-Shoup encryption

Alice

Gen: $(q, g_1, g_2) \leftarrow \mathcal{G}(1^n)$

$sk = (x_1, x_2, y_1, y_2, z) \leftarrow \mathbb{Z}_q$

$c := g_1^{x_1} g_2^{x_2}, d := g_1^{y_1} g_2^{y_2}$

$h := g_1^z$

for $m \in G$: get $r \leftarrow \mathbb{Z}_q$

$u_1 := g_1^r, u_2 := g_2^r, e := h^r m$

$\alpha := H(u_1, u_2, e), v := c^r d^{r\alpha}$

$\text{Enc}_{pk}(m) = (u_1, u_2, e, v)$

$pk = (g_1, g_2, c, d, h, H)$

$\xrightarrow{\hspace{2cm}}$

(u_1, u_2, e, v)

Bob

$\alpha := H(u_1, u_2, e)$

$$u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} = \begin{cases} \text{verified}, & v \\ \text{abort}, & \text{otherwise} \end{cases}$$

$\text{Dec}_{sk}(u_1, u_2, e, v) = e / u_1^z$

Cramer-Shoup encryption

Correctness:

1. $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = u_1^{x_1} u_2^{x_2} u_1^{y_1\alpha} u_2^{y_2\alpha} = g_1^{rx_1} g_2^{rx_2} g_1^{ry_1\alpha} g_2^{ry_2\alpha} = (g_1^{x_1} g_2^{x_2})^r (g_1^{y_1} g_2^{y_2})^{r\alpha} = c^r d^{r\alpha} = v$

Cramer-Shoup encryption

Correctness:

1. $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = u_1^{x_1} u_2^{x_2} u_1^{y_1\alpha} u_2^{y_2\alpha} = g_1^{rx_1} g_2^{rx_2} g_1^{ry_1\alpha} g_2^{ry_2\alpha} = (g_1^{x_1} g_2^{x_2})^r (g_1^{y_1} g_2^{y_2})^{r\alpha} = c^r d^{r\alpha} = v$
2. Since $u_1^z = h^r$, $\mathrm{Dec}_{sk}(u_1, u_2, e, v) = e/u_1^z = e/h^r = m$

Theorem

Cramer-Shoup is CCA2-secure

The Cramer-Shoup cryptosystem is CCA2-secure assuming that
(1) we have a universal one-way hash function H, and
(2) the Decisional Diffie-Hellman Problem is hard in the group G.

Theorem

Cramer-Shoup is CCA2-secure

The Cramer-Shoup cryptosystem is CCA2-secure assuming that
(1) we have a universal one-way hash function H, and
(2) the Decisional Diffie-Hellman Problem is hard in the group G.

Proof by reduction: Assuming that there is an adversary that can break the cryptosystem, and that the hash family is universal one-way, we can use this adversary to solve the Decisional Diffie-Hellman Problem.

Proof of Security

$\mathcal{S}$

$(g_1, g_2, u_1, u_2) \leftarrow \mathfrak{D}$ or $\mathfrak{R}$

$(x_1, x_2, y_1, y_2, z_1, z_2) \leftarrow \mathbb{Z}_q$

$m_0, m_1 \in G$

$c := g_1^{x_1} g_2^{x_2}, d := g_1^{y_1} g_2^{y_2}, h := g_1^{z_1} g_2^{z_2}$

$b \leftarrow \{0, 1\}$

$e := u_1^{z_1} u_2^{z_2} m_b, \alpha := H(u_1, u_2, e)$

$v = u_1^{x_1 + y_1 \alpha} u_2^{x_2 + y_2 \alpha}$

$c* = (u_1, u_2, e, v)$

$\mathcal{A}$

$\mathrm{Dec}_{sk}(c*) = e / u_1^{z_1} u_2^{z_2} = m_{b'}$

$$\begin{cases} \text{output b'}, & \mathfrak{D} \\ \perp, & \mathfrak{R} \end{cases}$$

$$\text{output} = \begin{cases} 1, & b = b' \\ 0, & b \neq b' \end{cases}$$

Comparison

- One of the few CCA2-secure cryptosystems that do not require zero-knowledge proofs or the random oracle

Comparison

- One of the few CCA2-secure cryptosystems that do not require zero-knowledge proofs or the random oracle
- Computationally efficient, esp. when using hybrid encryption

Comparison

- One of the few CCA2-secure cryptosystems that do not require zero-knowledge proofs or the random oracle
- Computationally efficient, esp. when using hybrid encryption
- Intractability assumptions are minimal (only DDH & hash)

Computation

The ciphertext is about four times plaintext (not a big deal in most applications) and takes about twice as much computation as ElGamal.

Cramer-Shoup encryption

Alice

Gen: $(q, g_1, g_2) \leftarrow \mathcal{G}(1^n)$

$sk = (x_1, x_2, y_1, y_2, z) \leftarrow \mathbb{Z}_q$

$c := g_1^{x_1} g_2^{x_2}, d := g_1^{y_1} g_2^{y_2}$

$h := g_1^z$

for $m \in G$: get $r \leftarrow \mathbb{Z}_q$

$u_1 := g_1^r, u_2 := g_2^r, e := h^r m$

$\alpha := H(u_1, u_2, e), v := c^r d^{r\alpha}$

$\text{Enc}_{pk}(m) = (u_1, u_2, e, v)$

$$\xrightarrow[(u_1, u_2, e, v)]{pk = (g_1, g_2, c, d, h, H)}$$

Bob

$\alpha := H(u_1, u_2, e)$

$$u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = \begin{cases} \text{verified}, & v \\ \text{abort}, & \text{otherwise} \end{cases}$$

$\text{Dec}_{sk}(u_1, u_2, e, v) = e/u_1^z$

Outline

Ronald Cramer

1968*, Dutch
Professor at the Centrum Wiskunde & Informatica (CWI) in Amsterdam and the University of Leiden
ETH Zurich, Institute for Theoretical Computer Science

Ronald Cramer

1968*, Dutch
Professor at the Centrum Wiskunde & Informatica (CWI) in Amsterdam and the University of Leiden
ETH Zurich, Institute for Theoretical Computer Science
hangs around in bars

Victor Shoup

born ?, USA
Professor at the Courant Institute of Mathematical Sciences (NYU)
IBM Zurich Research Laboratory

Victor Shoup

born ?, USA
Professor at the Courant Institute of Mathematical Sciences (NYU)
IBM Zurich Research Laboratory
on RateMyProfessors, he has an average rating of 1.4/5

Schneier on Cramer-Shoup

"If, in a few years, Cramer-Shoup still looks secure, cryptographers may look at using it instead of other defenses they are already using. But since IBM is going to patent Cramer-Shoup, probably not." [3]

Outline

Summary

Summary

- The Cramer-Shoup system is an asymmetric key encryption algorithm based on the ElGamal scheme
- First efficient scheme proven to be secure against adaptive chosen ciphertext attacks

thank you!

References

Mihir Bellare and Amit Sahai.
Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization.
In *Advances in cryptology—CRYPTO'99*, pages 519–536. Springer, 1999.

Ronald Cramer and Victor Shoup.
A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack.
In *Advances in Cryptology—CRYPTO'98*, pages 13–25. Springer, 1998.

Bruce Schneier.
Cramer-Shoup cryptosystem.
Crypto-Gram Newsletter, 15.09.98.