The Cramer-Shoup Cryptosystem

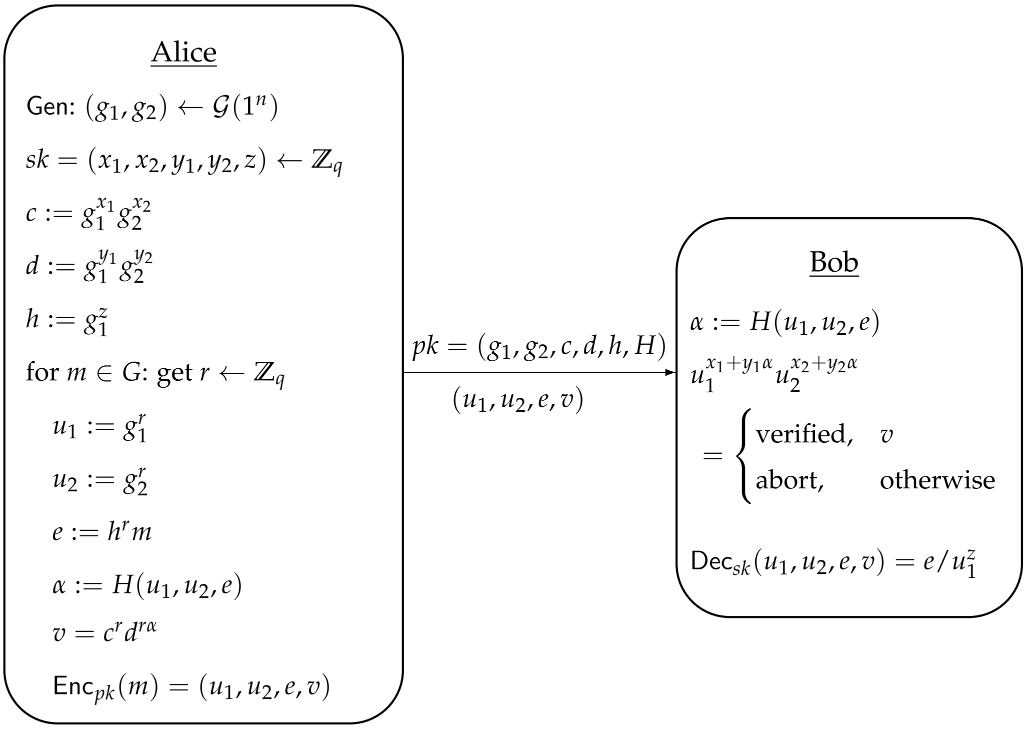
Eileen Wagner, 22.10.14

1 The Encryption Scheme

Definition An *adaptive chosen ciphertext attack* is an interactive chosen-ciphertext attack in which the adversary may send a number of ciphertexts to be decrypted, and use the results of these decryptions to select subsequent ciphertexts. Security against such CCA2-attacks is provably equivalent to non-malleability [1].

2 The Encryption Scheme

Take a random cyclic group G of order q, and a collision-resistant hash function H.



Alice

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

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

$c := g_1^{x_1} g_2^{x_2}$

$d := g_1^{y_1} g_2^{y_2}$

$h := g_1^z$

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

$u_1 := g_1^r$

$u_2 := g_2^r$

$e := h^r m$

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

$v = c^r d^{r\alpha}$

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

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

(u_1, u_2, e, v)

Bob

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

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

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

Correctness:

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

Since $u_1^z = h^r$, $\mathsf{Dec}_{sk}(u_1, u_2, e, v) = e/u_1^z = e/h^r = m$.

3 Security

Theorem The Cramer-Shoup cryptosystem is secure against adaptive chosen ciphertext attack assuming that (1) the hash function H is chosen from a universal one-way family, and (2) the Diffie-Hellman decision problem is hard in the group G. [2]

Proof via reduction.

4 Relevance

1. Security against adaptive chosen ciphertext attack (IND-CCA2) is currently the *strongest* notion of security
2. One of the few CCA2-secure cryptosystems that do not require zero-knowledge proofs or the random oracle
3. Computationally efficient, esp. when using hybrid encryption

Despite its advantages, Cramer-Shoup has not replaced padded RSA+OAEP, as Schneier has predicted:

> "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]

References

[1] 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.

[2] 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.

[3] Bruce Schneier. Cramer-Shoup cryptosystem. *Crypto-Gram Newsletter*, 15.09.98.