David Pointcheval
Yi Mu
Kefei Chen (Eds.)

Cryptology and Network Security

LNCS 4301

5th International Conference, CANS 2006
Suzhou, China, December 2006
Proceedings

Springer

David Pointcheval Yi Mu
Kefei Chen (Eds.)

Cryptology and Network Security

5th International Conference, CANS 2006
Suzhou, China, December 8-10, 2006
Proceedings

Springer

Volume Editors

David Pointcheval
CNRS, École Normale Supérieure
Paris, France
E-mail: David.Pointcheval@ens.fr

Yi Mu
Center for Information Security Research
SITACS, University of Wollongong
Wollongong NSW 2522, Australia
E-mail: ymu@uow.edu.au

Kefei Chen
Dept. of Computer Science and Engineering
Shanghai Jiaotong University
Shanghai 200240, P.R., China
E-mail: kfchen@sjtu.edu.cn

Library of Congress Control Number: 2006937156

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49462-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49462-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11935070 06/3142 5 4 3 2 1 0

Preface

The fifth International Conference on Cryptology and Network Security (CANS 2006) was held in Suzhou, Jiangsu, China, December 8–10, 2006. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR) and the National Nature Science Foundation of China (NSFC).

The 1st International Workshop on Cryptology and Network Security was held in Taipei, Taiwan, 2001. The second one was in San Francisco, California, USA, September 26-28, 2002, the third in Miami, Florida, USA, September 24-26, 2003, and the fourth in Xiamen, Fujian Province, China, December 14-16, 2005. CANS 2005 was the first CANS with proceedings published in the *Lecture Notes in Computer Science* series by Springer and granted the success of last year and this year, CANS 2006 was also published in the same series. The Program Committee received 148 submissions, and accepted 26 papers, all included in the proceedings.

The reviewing process, which took eight weeks, was run using the iChair software, written by Thomas Baignères and Matthieu Finiasz (EPFL, Switzerland). Each paper was carefully evaluated by at least three members from the Program Committee. We appreciate the hard work of the members of the Program Committee and external referees who gave many hours of their valuable time.

Note that these proceedings contain the revised versions of the selected papers. Since the revisions were not checked again before publication, the authors (and not the committee) bear full responsibility of the contents of their papers.

In addition to the contributed papers, there were two invited talks: Moni Naor and Xiaoyun Wang.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank the General Chair, Kefei Chen, the Co-chairs of the Organizing Committee Dong Zheng and Weidong Qiu, and people from the Shanghai Jaotong University for their time and efforts.

Finally, we wish to thank all the authors who submitted papers, and the authors of accepted papers for sending their final versions on time.

December 2006

David Pointcheval
Yi Mu
Kefei Chen

Fifth International Conference on Cryptology and Network Security (CANS 2005)

In Cooperation with
The International Association for Cryptologic Research (IACR)

Sponsored by
Shanghai Jiao Tong University (SJTU), China
National Nature Science Foundation of China (NSFC)

General Chair

Kefei Chen	Shanghai Jaotong University, China

Program Chairs

Yi Mu	University of Wollongong, Australia
David Pointcheval	CNRS and ENS, France

Program Committee

Farooq Anjum	Telcordia, USA
Feng Bao	Institute for Infocomm Research, Singapore
Christophe Bidan	Supélec, France
John Black	University of Colorado, USA
Carlo Blundo	Università di Salerno, Italy
Colin Boyd	QUT, Australia
Xavier Boyen	Voltage, USA
Laurent Bussard	EMIC, Germany
Liqun Chen	HP Laboratories, UK
Anand Desai	NTT MCL, USA
Cunsheng Ding	Hong Kong Univ. Sci. Tech., China
Steven Galbraith	Royal Holloway Univ. of London, UK
Marc Girault	France Telecom, France
Nick Howgrave-Graham	NTRU Cryptosystems, USA
Marc Joye	Thomson R&D, France
Kwangjo Kim	ICU, South Korea
Kaoru Kurosawa	Ibaraki University, Japan
Xuejia Lai	Shanghai Jiao Tong University, China
Dong Hoon Lee	Korea University, South Korea
Arjen Lenstra	EPFL, Switzerland

Javier Lopez	University of Malaga, Spain
Atsuko Miyaji	JAIST, Japan
David Naccache	ENS and University of Paris II, France
Kaisa Nyberg	TU of Helsinki and Nokia, Finland
Giuseppe Persiano	Università di Salerno, Italy
Josef Pieprzyk	Macquarie University, Australia
C.-Pandu Rangan	Indian Institute of Technology, India
Kazue Sako	NEC, Japan
Berry Schoenmakers	TU Eindhoven, Netherlands
Willy Susilo	University of Wollongong, Australia
Vijay Varadharajan	Macquarie University, Australia
Xiaofeng Wang	Indiana University, USA
Duncan Wong	City University of Hong Kong, China
Chaoping Xing	National Univ. of Singapore, Singapore
Shouhuai Xu	University of Texas, USA
Sung-Ming Yen	National Central Univ., Taiwan

Organizing Committee

Dong Zheng (Chair)	Shanghai Jiaotong University, China
Weidong Qiu (Chair)	Shanghai Jiaotong University, China
Zheng Huang	Shanghai Jiaotong University, China
Shengli Liu	Shanghai Jiaotong University, China
Jie Guo	Shanghai Jiaotong University, China

External Referees

Patrick Amon
Toshinori Araki
Roberto Avanzi
Pedro Bados Aguilar
Chris Charnes
Jing Chen
Xiaofeng Chen
Benoît Chevallier-Mames
Bessie C. Hu
Carlos Cid
Yang Cui
Paolo D'Arco
Alex Dent
Hiroshi Doi
Gerardo Fernandez
Jun Furukawa
Clemente Galdi
Changzhe Gao
Juan Gonzalez
Vanessa Gratzer
Gaurav Gupta
Goichiro Hanaoka
Matt Henricksen
Guillaume Hiet
Paul Hoffman
Chao-Chih Hsu
Xinyi Huang
Toshiyuki Isshiki
Erhan Kartaltepe
Hiroaki Kikuchi
Mehmet Kiraz
Yuichi Komano
Jérôme Lebègue
Tieyan Li
Zhuowei Li
Benoît Libert
Wei-Chih Lien
Hsi-Chung Lin
Liang Lu
Ludovic Mé
Miao Ma
Frédéric Majorczyk
Toshihiko Matsuo
Krystian Matusiewicz
Kengo Mori
Benjamin Morin
Sean Murphy
Satoshi Obana

Tatsuaki Okamoto
Dag Arne Osvik
Dan Page
Pascal Paillier
Kenny Paterson
Rodrigo Roman
Nicholas Sheppard
Martijn Stam
Ye Tang
Christophe Tartary
Isamu Teranishi
Xiaojian Tian
Rafael Timóteo de Sousa Júnior
Eric Totel
Udaya Kiran Tupakula
Lionel Victor
Jos Villegas
Ivan Visconti
Kumar Viswanath
Huaxiong Wang
William Whyte
Robert W. Zhu
Shidi Xu
Guomin Yang
Dennis Y. W. Liu
Bo Zhu

Table of Contents

Encryption

Key Exchange

Authentication and Signatures

Proxy Signatures

Cryptanalysis

Implementation

Steganalysis and Watermarking

Boolean Functions and Stream Ciphers

Intrusion Detection

Disponibility and Reliability

Concrete Chosen-Ciphertext Secure Encryption from Subgroup Membership Problems

Jaimee Brown, Juan Manuel González Nieto, and Colin Boyd

Information Security Institute
Queensland University of Technology
Brisbane, Australia
{j2.brown, j.gonzaleznieto, c.boyd}@qut.edu.au

Abstract. Using three previously studied subgroup membership problems, we obtain new concrete encryption schemes secure against adaptive chosen-ciphertext attack in the standard model, from the Cramer-Shoup and Kurosawa-Desmedt constructions. The schemes obtained are quite efficient. In fact, the Cramer-Shoup derived schemes are more efficient than the previous schemes from this construction, including the Cramer-Shoup cryptosystem, when long messages are considered. The hybrid variants are even more efficient, with a smaller number of exponentiations and a shorter ciphertext than the Kurosawa-Desmedt Decisional Diffie-Hellman based scheme.

Keywords: public key encryption, chosen ciphertext security, Cramer-Shoup framework, subgroup membership problems, hybrid encryption.

1 Introduction

The underlying security goal for a public key encryption scheme is to guarantee that no partial information about a plaintext message is revealed from its ciphertext, a notion often called indistinguishability of encryptions. Indistinguishability against adaptive chosen ciphertext attack (IND-CCA), where an adversary is given the capability to decrypt ciphertexts of his choice, with the exception of a target ciphertext, is considered to be the correct notion of security for general-purpose public key encryption schemes. We shall refer to schemes that achieve this level of security as CCA-secure schemes.

We present several practical, concrete encryption schemes that are proven CCA-secure in the standard model each based on the difficulty of a particular subgroup membership problem. Several of these schemes are more efficient than previous CCA-secure schemes, and all schemes rely on different problems than have previously been used for CCA-schemes. We have used three subgroup membership problems previously studied in the literature: the subgroup membership problem discussed by González-Nieto, Boyd and Dawson [6], the r-th residue problem [8], and Okamoto and Uchiyama's [9] p-subgroup problem.

Cramer and Shoup [1] proposed the first encryption scheme that was simultaneously practical and CCA-secure under standard intractability assumptions. Cramer and Shoup [3] later generalised their encryption scheme to give a

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 1–18, 2006.

framework for constructing CCA-secure encryption schemes from general subgroup membership problems and *hash proof systems* (HPS). Accompanying their framework, Cramer and Shoup also described three instantiations of the framework using three subgroup membership problems, namely Decisional Diffie-Hellman, Decisional Composite Residuosity [10] and the classical Quadratic Residuosity problem. Kurosawa and Desmedt [7] later presented an efficient hybrid encryption scheme based on the Cramer-Shoup cryptosystem, as well as a generalised construction of CCA-secure hybrid encryption schemes from the HPS primitive introduced by Cramer and Shoup.

Motivation and Contribution. The Cramer-Shoup construction is an important development in the area of chosen-ciphertext security for public key encryption. However, their general construction is quite complicated, and developing schemes requires a strong understanding of how the construction works, and the steps involved applying it concretely. We believe that understanding in this case is best achieved through example, and our hope is that by applying the construction to a number of different subgroup membership problems, and detailing the steps taken, the process of deriving new schemes will become clearer.

Of independent interest are the actual schemes obtained by applying both the Cramer-Shoup and Kurosawa-Desmedt to the three previously proposed subgroup membership problems. For the Cramer-Shoup construction, the resulting encryption schemes are in fact more efficient than the schemes presented by Cramer and Shoup, including the Cramer-Shoup cryptosystem, when the encryption of long messages is considered. The hybrid schemes obtained by applying the Kurosawa-Desmedt construction to the same subgroup membership problems, are even more efficient. In fact, the number of exponentiations and the size of the ciphertexts are smaller than the previous DDH-based hybrid scheme.

Related Work. Gjøsteen [5] discussed symmetric subgroup membership (SSM) problems and described an instantiation of the Cramer-Shoup framework specific for such problems. A symmetric subgroup membership problem considers a group X and non-trivial subgroups L and $\tilde{L}$ such that $X = L\tilde{L}$, $L \cap \tilde{L} = \{1\}$. It is said to be hard if distinguishing elements of L from elements of $X \backslash L$, and elements of $\tilde{L}$ from elements of $X \backslash \tilde{L}$ are both hard problems. Gjøsteen also showed that the decisional Diffie-Hellman (DDH) problem and the symmetric subgroup membership problem are related such that SSM is not harder than DDH. In other words, the difficulty of SSM implies the difficulty of DDH. Although Gjøsteen showed the general encryption scheme for SSMs, we analyse instances of subgroup membership problems and the resulting concrete schemes obtained.

2 Preliminaries

If x is an integer, we denote the bit length of x as $|x|$. For a set S, we denote the order of S as $|S|$. We denote by $x \in_R S$ the act of sampling x from S uniformly at random. The notation G_α is used to denote a group of order α.

We say that two distributions X and Y on a set S are β-close if the distance between them is at most β. The distance between distributions X and Y is defined as

$$Dist(X, Y) = \frac{1}{2} \sum_{s \in S} |Pr[X = s] - Pr[Y = s]|.$$

3 Chosen-Ciphertext Security

3.1 The Cramer-Shoup Construction

Cramer and Shoup introduced the notions of universal projective hash families and universal hash proof systems. Let us now summarise the main notions and definitions from Cramer and Shoup's work. For further details, we refer the reader to the full version of their paper [2].

A hash proof system relies on a finite set X, or more formally a distribution on sets, a subset $L \subset X$ with an associated witness set W and a relation $R \subset X \times W$. A pair $(x, w) \in R$ allows one to show that an element $x \in X$ is also in L. We say that $w \in W$ is a witness for $x \in L$. The underlying assumption is that it is infeasible to distinguish between a random element in L and a random element in $X \backslash L$. This is called the *subset membership problem.*

The hash proof system associates an instance of a subset membership problem with a family of keyed hash functions H that operate on X, called a *projective hash family.* It is required that given a hash key k and an element $x \in X$, the value of the function $H_k(x)$ can be computed. It is also required that this family of functions be *projective*, that is, given only an additional key $\alpha(k)$ and a subgroup element $x \in L$, the value $H_k(x)$ is uniquely determined. Moreover, it is a requirement that given $\alpha(k)$ and a pair $(x, w) \in R$, that $H_k(x)$ can be computed efficiently (without k). The hash proof system also requires that hash keys and witness elements can be efficiently sampled uniformly (or close to uniformly) from the hash key set K and the witness set W, respectively.

Let $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ be such a projective hash family, where K, Π and S are finite sets, and X and L are also finite sets as defined above. The functions H and α are defined such that $H_{k \in K} : X \to \Pi$ and $\alpha : K \to S$.

A projective hash family is ϵ-*universal* if given the projection key $s = \alpha(k)$, even though $H_k(x)$ is completely determined for $x \in L$, for any $x \in X \backslash L$, one can guess $H_k(x)$ with probability at most ϵ (without knowledge of k).

A projective hash family is ϵ-*universal*$_2$ if given $s = \alpha(k)$ and $H_k(x^*)$ for some $x^* \in X \backslash L$, even though $H_k(x)$ is completely determined for $x \in L$, for any $x \in X \backslash L$, one can guess $H_k(x)$ with probability at most ϵ (without knowledge of k).

A projective hash family is ϵ-*smooth* if the distributions $U = (x, s, \pi')$, $V = (x, s, \pi)$, where $x \in_R X \backslash L$, $s = \alpha(k)$ for $k \in_R K, \pi' \in_R \Pi, \pi = H_k(x)$, are ϵ-close.

It is also useful to describe an *extended* hash proof system, which associates the subset membership problem with a projective hash family $\hat{\mathbf{H}} = (H, K, X \times E, L \times E, \Pi, S, \alpha)$ for a finite set E.

A hash proof system is *strongly* universal (respectively, universal$_2$, smooth) if the associated projective hash family is also ϵ-universal (respectively, ϵ-universal$_2$, ϵ-smooth) for negligible ϵ, or more formally $\epsilon(\ell)$ is a negligible function in security parameter ℓ.

The Cramer-Shoup framework constructs a CCA-secure encryption scheme given a ϵ-smooth hash proof system $\mathbf{P}$ with associated projective hash family $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$, and a $\hat{\epsilon}$-universal$_2$ extended hash proof system $\hat{\mathbf{P}}$ with associated projective hash family $\hat{\mathbf{H}} = (\hat{H}, \hat{K}, X \times \Pi, L \times \Pi, \hat{\Pi}, \hat{S}, \hat{\alpha})$ for the subset membership problem (X, L, W, R), where ϵ and $\hat{\epsilon}$ are negligible (or more formally, negligible functions of the security parameter). The construction requires that Π is an abelian group, which we will notate additively in the encryption scheme below. Note also that the message space is Π.

Key Generation

1. $k \in_R K, \hat{k} \in_R \hat{K}$
2. $s = \alpha(k) \in S$
3. $\hat{s} = \hat{\alpha}(\hat{k}) \in S$
4. pk $= (s, \hat{s})$.
5. sk $= (k, \hat{k})$.

Encryption of $m \in \Pi$

1. $(x, w) \in_R R$
2. $\pi = H_k(x) \in \Pi$ given (s, x, w)
3. $e = m + \pi \in \Pi$.
4. $\hat{\pi} = \hat{H}_{\hat{k}}(x, e) \in \hat{\Pi}$ given (s, x, e)
5. ciphertext is $(x, e, \hat{\pi})$

Decryption of $(x, e, \hat{\pi})$

1. $\hat{\pi}' = \hat{H}_{\hat{k}}(x, e) \in \hat{\Pi}$ given (x, e, k)
2. if $\hat{\pi} \neq \hat{\pi}'$ then halt
3. $\pi = H_k(x) \in \Pi$ given (x, k)
4. $m = e - \pi \in \Pi$

Cramer and Shoup show that if there exists an adversary that has non-negligible advantage in an adaptive chosen ciphertext attack, then a distinguisher for L that has non-negligible advantage can be constructed. In other words, they show that the above scheme is secure against adaptive chosen ciphertext attack provided that the underlying subset membership problem is hard.

3.2 The Kurosawa-Desmedt Hybrid Construction

Kurosawa and Desmedt [7] showed that a hash proof system that associates a subset membership problem with a strongly universal$_2$ projective hash family can be used to construct efficient hybrid encryption schemes. Let $\mathbf{P}$ be a hash proof system that associates the strongly universal$_2$ projective hash family $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ with the subset membership problem (X, L, W, R). Let $SKE = (E, D)$ be a semantically secure symmetric-key encryption scheme, let MAC be a one-time secure message authentication code, and KDF a key derivation function (whose output is hard to distinguish from random). Kurosawa and Desmedt prove that the following hybrid encryption schemes is CCA-secure.

Key Generation

1. $k \in_R K$
2. $s = \alpha(k) \in S$
3. $pk = s$.
4. $sk = k$.

Encryption of $m \in \Pi$

1. $(x, w) \in_R R$
2. $\pi = H_k(x) \in \Pi$ given (s, x, w)
3. $(K', K) = KDF(\pi)$
4. $\chi = E_K(m)$
5. $t = MAC_{K'}(\chi)$
6. ciphertext is (x, χ, t)

Decryption of (x, χ, t)

1. $\pi = H_k(x)$ given (x, k)
2. $(K', K) = KDF(\pi)$
3. If $t \neq MAC_{K'}(\chi)$ then *halt*
4. $m = D_K(\chi)$

A concrete hybrid encryption scheme based on the HPS used to construct the Cramer-Shoup cryptosystem was proposed and proven secure under the Decisional Diffie-Hellman assumption when used with information theoretic KDF and MAC. Gennaro and Shoup [4] later showed that relying on these information theoretic tools eliminates the efficiency gain of the hybrid scheme versus the original Cramer-Shoup scheme, and gave a different proof that instead relies on any computationally secure KDF and MAC.

4 Concrete CCA-Secure Schemes from Subgroup Membership Problems

We describe concrete encryption schemes obtained by applying the Cramer-Shoup and the Kurosawa-Desmedt constructions to three particular subgroup membership problems which have been studied previously in the literature.

4.1 The GBD Subgroup Membership Problem

The GBD cryptosystem [6] is semantically secure based on the difficulty of the following subgroup membership problem. Consider primes p,q_0,q_1 such that $p = 2N + 1$ where $N = q_0 q_1$ and $|q_0| = |q_1| = \lambda$. The set of quadratic residues modulo p is a cyclic subgroup of order N of the multiplicative group $\mathbb{Z}_p^*$. Let this group be X, and let L be the subgroup of X with order q_0. The GBD subgroup membership problem is to distinguish elements of L from elements of $X \backslash L$. We can also view these groups by considering that $\mathbb{Z}_p^*$ can be viewed as an internal direct product of subgroups:

$$\mathbb{Z}_p^* = G_{q_0} \cdot G_{q_1} \cdot T$$

where T is the subgroup $\{-1, 1\}$. Then $X = G_{q_0} \cdot G_{q_1}$ and $L = G_{q_0}$. Indeed this is an instance of the symmetric subgroup membership problem as discussed by Gjøsteen [5].

Constructing a CCA-secure Encryption Scheme. We now apply the Cramer-Shoup construction to this subgroup membership problem, which is also the application of the Gjøsteen's construction [5]. To find a generator g for L, one can select μ at random from $\mathbb{Z}_p^*$ and compute $g = \mu^{2q_1}$. It will be a generator with overwhelming probability. Let $W_* = \{0, ..., q_0 - 1\}$. One can sample an element x from L with a corresponding witness $w \in W$ by choosing w at random in W and computing $x = g^w$. However, in practice q_0 is kept private and w must instead be selected from $W = \{0, ..., N - 1\}$.

Now, let $K = \{0, ..., N - 1\}$ and define $H_{k \in K}(x) = x^k$ and $\alpha(k) = H_k(g)$. Hence $\Pi = X$ and $S = L$. It is easy to see that $\mathbf{H} = (H, K, X, L, X, L, \alpha)$ is projective since given $s = \alpha(k) = g^k$ and $x = g^w$, $H_k(x) = x^k = s^w$ is uniquely determined. By Lemma 1 in [5], $\mathbf{H}$ is $1/q_1$-smooth. Since K can be sampled uniformly, and the required algorithms for computing H_k are available, we have a strongly smooth hash proof system $\mathbf{P}$ that associates the GBD subgroup membership problem with $\mathbf{H}$ when q_1 is large.

To obtain a strongly universal$_2$ hash proof system $\hat{\mathbf{P}}$, let us first suppose that for some sufficiently large n, there is an available injective function $\Gamma : X \times X \rightarrow R^n$ for $\mathrm{R} = \{0, ..., 2^\lambda - 1\}$. Consider the extended projective hash family $\hat{\mathbf{H}} = (\hat{H}, K^{n+1}, X \times X, L \times X, X, L^{n+1}, \hat{\alpha})$ where for $(\tilde{k}, \hat{k}_1, ..., \hat{k}_n) \in K^{n+1}$ and $(\gamma_1, ..., \gamma_n) = \Gamma(x, e)$, where we define

- $\hat{H}_{\tilde{k},\hat{k}_1,...,\hat{k}_n}(x, e) = H_{\tilde{k}}(x) \prod_{i=1}^n H_{\hat{k}_i}(x)^{\gamma_i} = x^{\tilde{k}+\sum_{i=1}^n \hat{k}_i \gamma_i}$
- $\hat{\alpha}(\tilde{k}, \hat{k}_1, ..., \hat{k}_n) = (\alpha(\tilde{k}), \alpha(\hat{k}_1), ..., \alpha(\hat{k}_n)) = (g^{\tilde{k}}, g^{\hat{k}_1}, ..., g^{\hat{k}_n})$

By theorem 3 in [3], $\hat{\mathbf{H}}$ is $1/q_1$-universal$_2$. It is easy to show that the required algorithms are available for the resulting strongly universal$_2$ hash proof system $\hat{\mathbf{P}}$ for $\hat{\mathbf{H}}$. We now have what is necessary to build a CCA-secure encryption scheme based on this problem.

Since we now have a strongly smooth HPS $\mathbf{P}$, and a strong universal$_2$ HPS $\hat{\mathbf{P}}$, applying the Cramer-Shoup construction will give us a CCA-secure encryption scheme. However, to improve efficiency, we can replace the injective function $\Gamma : X \times X \rightarrow R^n$ by a collision resistant hash function $h : X \times X \rightarrow \{0, 1\}^m$ (such as SHA-1 where $m = 160$) so that the n can be much smaller. Indeed, we can choose $n = 1$ and the resulting scheme will still be secure against chosen-ciphertext attack. The resulting encryption scheme is as follows:

The CS-GBD encryption scheme. For the description below, $p = 2N+1$ is prime where $N = q_0 q_1$ for primes q_0, q_1 of bit length λ. Let h be a collision resistant hash function.

Key Generation

1. Choose $p = 2q_0q_1 + 1$
2. $\mu \in_R \mathbb{Z}_p$
3. $g = \mu^{2q_1}$
4. $k, \tilde{k}, \hat{k} \in_R \mathbb{Z}_N$
5. $s = g^k$, $\tilde{s} = g^{\tilde{k}}$, $\hat{s} = g^{\hat{k}}$
6. $pk = (p, g, s, \tilde{s}, \hat{s})$
7. $sk = (q_0, k, \tilde{k}, \hat{k})$

Encryption of $m \in X$

1. $w \in_R \{0, ..., N-1\}$
2. $x = g^w$
3. $\pi = s^w$
4. $e = m\pi$
5. $\hat{\pi} = \tilde{s}^w \hat{s}^{h(x,e)w}$
6. Ciphertext is $(x, e, \hat{\pi})$

Decryption of $(x, e, \hat{\pi})$

1. $\hat{\pi}' = x^{\tilde{k}+h(x,e)\hat{k}}$
2. If $\hat{\pi} \neq \hat{\pi}'$, then halt
3. $\pi = x^k$
4. $m = e/\pi$

Note that we are implicitly assuming that $(x, e, \hat{\pi}) \in X^3$, so the decryption algorithm should check that $(\frac{x}{p}) = (\frac{e}{p}) = 1$ and reject otherwise. This check can be performed at low cost using an efficient algorithm for computing Jacobi symbols.

Security of CS-GBD. For a probabilistic polynomial-time adversaries A, A', let $Adv_{A,CS-GBD}^{CCA}$ be A's advantage in an adaptive chosen ciphertext attack, and let $Adv_{A'}^{GBD}$ be the advantage of A' in distinguishing subgroup elements from non-subgroup elements. Let Q be the number of decryption queries allowed by A. Also, let δ_{tcr} be the probability of finding a collision for the hash function h for input (x, e).

Theorem 1. *If the GBD subgroup membership problem is hard, and the hash function h is a collision resistant hash function, the CS-GBD is secure against adaptive chosen ciphertext attack. In particular, for all adversaries A, there exists a probabilistic polynomial-time algorithm A′ such that*

$$Adv^{CCA}_{A,CS-GBD} \leq Adv^{GBD}_{A'} + (Q+1)/q_1 + \delta_{tcr} \tag{1}$$

Proof. We consider a simulator A' that interacts with a chosen-ciphertext adversary A against CS-GBD in the following way.

1. Given input (p, g) and target element $x^* \in X$.
2. Run the Key Generation algorithm to get (pk, sk) and gives the pk to A
3. Answer A's decryption queries $(x, e, \hat{\pi})$ by running decryption algorithm
4. When A outputs messages m_0, m_1:
   (a) Flip coin $b \in_R \{0, 1\}$
   (b) Compute $\pi^* = H_k(x^*)$
   (c) Compute $e^* = \pi^* m_b$
   (d) Compute $\hat{\pi}^* = \hat{H}_k(x^*, e^*)$
   (e) Give A challenge ciphertext $(x^*, e^*, \hat{\pi}^*)$
5. Answer A's decryption queries $(x, e, \hat{\pi}) \neq (x^*, e^*, \hat{\pi}^*)$ by running decryption algorithm
6. When A output guess bit b', output 1 if $b = b'$. Otherwise output 0.

We want to consider the behaviour this simulator in two different cases: when $x^* \in L$ and when $x^* \notin L$. Let T' be the event that the simulator outputs 1 in the former case, and let T' be the event that it outputs 1 in the latter case. The advantage that A' has in distinguishing the subgroup membership of x^* is

$$Adv^{GBD}_{A'} = |\Pr[T] - \Pr[T']| \tag{2}$$

Let $Adv^{CCA}_{A,CS-GBD}$ be the adversary's advantage in an adaptive chosen ciphertext attack against CS-GBD. Our goal is to show that if $Adv^{GBD}_{A'}$ is negligible, then $Adv^{CCA}_{A,CS-GBD}$ will also be negligible.

When $x^* \in L$, the simulation provided by the simulator to the adversary is perfect. Therefore, we have

$$Adv^{CCA}_{A,CS-GBD} \leq |\Pr[T'] - 1/2| \tag{3}$$

When $x^* \notin L$, we must analyse the behaviour more closely. To do so, we describe a sequence of simulators that contain modifications of the previous simulators. In the following analysis, we denote T_i as the event that the simulator i outputs a 1.