Provable Partial Key Escrow

Kooshiar Azimian [*]
Electronic Research Center, Sharif University of Technology, and
Computer Engineering Department, Sharif University of Technology
Tehran, Iran
Email: Azimian@ce.sharif.edu

Javad Mohajeri [*]
Electronic Research Center, Sharif University of Technology
Tehran, Iran
Email: Mohajer@sharif.edu

Mahmoud Salmasizadeh [*]
Electronic Research Center, Sharif University of Technology
Tehran, Iran
Email: salmasi@sharif.edu

Samuel S. Wagstaff, Jr. [†]
Center for Education and Research in Information Assurance and
Security, and Department of Computer Sciences, Purdue University
West Lafayette, IN 47907-1398 USA
Email: ssw@cerias.purdue.edu

Abstract. In this paper we first propose two new concepts concerning the notion of key escrow schemes: provable partiality and independence. Roughly speaking, a scheme has provable partiality if the existence of a polynomial time for recovering the secret from escrowed information implies there is a polynomial time algorithm for solving a well known intractable problem. A scheme is independent if the secret key and the escrowed information are independent. Finally, we propose a new verifiable partial key escrow scheme, based on McCurley's encryption scheme, satisfying both of the above criteria.

1 Introduction

A key escrow encryption scheme is a scheme in which a trusted third party (TTP) can decrypt cipher texts in special circumstances. The goal is to be able to retrieve important plain texts in case of key loss or refusal of a malicious user to decrypt a cipher text.

1.1 Partial Key Escrow (PKE)

The idea of partial key escrowing, presented first by Shamir in 1995, is to prevent the TTP from decrypting the cipher text immediately. Shamir proposed to give the TTP only the first eight bits of a 56-bit key. Then the TTP still must make a brute-force search of a key space of size 2^{48} to obtain the private key [Sh95]. It is easy to see that trying 2^{48} possible keys is not infeasible. However, it would be difficult to uncover many keys quickly and simultaneously with this system.

1.2 Verifiable Partial Key Escrow (VPKE)

When the TTP receives part of a key to escrow, he must be sure that the user has not cheated. That is, he must be able to verify that the secret key can be found in the expected time using the escrowed information. This is what is done by a VPKE scheme. The issue of verifiability was introduced independently by Micali [Mi95] and by Bellare and Goldwasser [BG95], who proposed the first VPKE schemes. Their schemes were based on Diffie-Hellman and RSA.

2 The New Properties

In this section we introduce two new properties and discuss their importance in key escrow schemes.

2.1 Provable Partiality

Partiality is an important property of a good key escrow scheme. As explained in [Sh95], [Mi95] and [BG95], it means that the TTP cannot uncover many keys simultaneously.

In [Mi95] Micali proposed a key escrow scheme based on Diffie-Hellman, and claimed that it had partiality because the fastest algorithm he knew to recover the key from escrow data took more than 2^{40} steps. However, the next year Van Oorschot and Wiener [WO96] discovered an algorithm that recovers the key from escrow data in far fewer than 2^{40} steps. Most VPKE schemes suffer from a similar weakness. They are supposed to have partiality if the proposed attack will take a long time using known algorithms. But it is possible that a new algorithm will allow a fast attack on the scheme.

Thus, the discovery of a new algorithm could break the partiality of a VPKE scheme. We introduce provable partiality in an effort to avoid this problem.

We say that a VPKE scheme is provably partial if any algorithm to break the scheme in polynomial time can be used to construct an algorithm for solving a problem well known to be intractable in polynomial time. Such intractable problems include NP-complete problems, of course, and also problems such as integer factoring and the discrete logarithm problem, which have been studied for a long time without the discovery of any tractable algorithm to solve them.

2.2 Independence

We say that a VPKE scheme is independent if the escrowed information and the secret are independent. This means that each user can change his secret without changing the escrowed information. This property allows each user to change his secret frequently without needing to report the change to the TTP. Independence makes the VPKE scheme more reliable and compatible. Furthermore, the frequent change of secret by a user greatly increases the computational difficulty faced by a dishonest TTP before it is officially requested (by the user or by a court order).

3 The New Scheme

Now we present a VPKE scheme having both provable partiality and independence.

3.1 The Encryption Scheme of McCurley

In his paper [Mc88] in which he proposes a new key distribution system, McCurley also presents an encryption scheme. This scheme is similar to the ElGamal cryptosystem, but works in a subgroup of $\mathbf{Z}_N^*$, where N is a composite number of special form. In McCurley's encryption scheme, each user A constructs a modulus $N = pq$, where p and q are large primes satisfying

- $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$,

- $(p-1)/2$ and $(q-1)/2$ are primes, and

- $(p+1)/4$ and $(q+1)/8$ have large prime factors.

Then A chooses a random number S modulo N and computes $y = 16^S \bmod N$. Finally, A makes y and N public and keeps p, q and S secret.

When B wishes to send a message m (a number modulo N) to A, B and A do the following:

- B chooses a random number k (modulo N), computes $u = 16^k \bmod N$ and $t = m \cdot y^k \bmod N$, and sends u and t to A.

- A decrypts the pair u, t by computing $m = t \cdot u^{-S} \bmod N$.

The proposed scheme is provable secure, based on the intractability of factoring integers [Sh85], [Mc88].

3.2 The New VPKE scheme

McCurley's encryption scheme has the nice property that each user has two independent secrets. One is the factorization of the modulus N. The other is the exponent S. We use this property to create a new key escrow scheme. The factorization of N (either p or q suffices, since N is public) is given to the TTP as the escrow data. The exponent S is kept secret.

Knowing the factorization of N, the TTP can break the system (find S and then recover m from u and t) by computing discrete logarithms modulo p and modulo q. If the parameters are chosen properly, it will be possible for the TTP to perform this computation once in a while, when it is requested to recover a secret, but not to do it frequently without a legitimate request. Currently, p and q should each have about 400 to 500 bits for this property to hold. This size should be increased as our ability to compute discrete logarithms improves. See [Po87] for a fast way to compute discrete logarithms.

4 The New System Advantages

The new system is a VPKE scheme because the TTP can verify the honesty of the user by testing whether the escrowed alleged factors of N really are factors of the public N. Moreover, the new scheme is a partial key escrow scheme because the secret exponent S is not given to the TTP.

In this section we show that the new system has both provable partiality and independence.

4.1 Provable Partiality

From [Mc88] we know that the existence of a polynomial time algorithm which can break the system using the factorization of N implies that there is a polynomial time algorithm to solve the discrete logarithm problem modulo a prime $\equiv 3 \pmod 4$. But this problem is considered to be intractable [Go93]. Therefore, the new scheme has provable partiality.

4.2 Independence

It is clear that the escrowed information—the factorization of the modulus N—and the secret exponent S are independent, at least if the approximate size of N is fixed. Thus, the user can change S at any time without changing N or reporting the change to the TTP. In former systems such as [Sh95], [Mi95] and [BG95], the escrowed data and the secret are related, so the user may not change the secret without communicating the change to the TTP.

5 Conclusion

We have proposed two new and useful properties of key escrowing. These properties make a key escrow system more reliable and compatible. Then we introduced a new VPKE scheme satisfying both new properties. The new system is based on McCurley's encryption scheme. The new scheme has high security and a reasonable secret recovery time.

References

[BG95]   M. Bellare and S. Goldwasser. Verifiable partial key escrow. *Proc. Fourth ACM Conf. on Computer and Communications Security*, April, 1997, pp. 78–91. Also Technical Report CS95-447, Department of CS and Engineering, UCSD, October 1995.

[Go93]   D. M. Gordon. Discrete logarithms in $GF(p)$ via the number field sieve. *SIAM J. Discrete Math.*, 16 (1993), pp. 124–138.

[Mc88]   K. McCurley. A key distribution system equivalent to factoring. *Journal of Cryptology*, 1 (1988), pp. 95–105.

[Mi95]   S. Micali. Guaranteed partial key escrow. MIT/LCS/TM-537, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 1995.

[Po87]   C. Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. In *Discrete Algorithms and Complexity*, pp. 119–143. Academic Press, 1987.

[Sh85]   Z. Shmuley. Composite Diffie-Hellman public key generating systems are hard to break. Technical Report 356, Computer Science Department, Technion, Israel, 1985.

[Sh95]   A. Shamir. Partial key escrow: A new approach to software key escrow. Private communication made at Crypto '95. Also presented at Key Escrow Conference, Washington, D.C., September 15, 1995.

[WO96] P. C. Van Oorschot and M. Wiener. On Diffie-Hellman key agreement with short exponents. *Advances in Cryptology—EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, U. Maurer, ed., pp. 332–343, Springer-Verlag, Berlin, 1996.