

A Range Test Secure in the Active Adversary Model

Kun Peng and Ed Dawson

Information Security Institute
Queensland University of Technology
126 Margaret St, Brisbane, QLD4000
Email: k.peng@qut.edu.au
<http://www.isi.qut.edu.au/people/pengk/>

Abstract

In ACISP 2006, Peng *et al* proposed a novel range test technique, which tests whether the integer encrypted in a ciphertext is in an interval range. Their solution is more efficient than any previous solution to range test. However, their technique only works in the passive adversary model, so cannot be widely applied. In this paper, the range test by Peng *et al* is optimised to be secure in the active adversary model. Although the new range test protocol is less efficient than the original scheme by Peng *et al*, it is still an efficient solution and can be employed in a much wider application area.

Keywords: range test, correctness, soundness, active adversary model

1 Introduction

Peng *et al* (Peng, Boyd, Dawson & Okamoto 2006) solved a cryptographic problem: range test. In a range test, one party (the tester) holds a ciphertext and wants to know whether the message encrypted in the ciphertext is within a certain interval range. Another party, called the decryption authority, holds the decryption key of the encryption system and is asked to help the tester. They run an interactive protocol to implement the range test. After the range test protocol, the decryption authority and the tester obtain no information related to the message encrypted in the ciphertext except the test result. Range test is useful in a wide range of cryptographic applications, where privacy of certain data must be maintained when they are processed. Peng *et al* (Peng et al. 2006) show that it is important in applications like electronic auction, electronic voting, electronic finance, group signature, publicly verifiable secret sharing and verifiable encryption. They define security of a range test as follows.

- **Correctness:** If the encrypted message is in the interval range, the test outputs TRUE.
- **Soundness:** If the test outputs TRUE, the encrypted message is in the interval range.
- **Privacy:** No information about the encrypted message is revealed except what can be deduced from the test result.

Copyright (c) 2007, Australian Computer Society, Inc. This paper appeared at the Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW), Ballarat, Australia. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 68. Ljiljana Brankovic, Paul Coddington, John F. Roddick, Chris Steketee, Jim Warren, and Andrew Wendelborn, Eds. Reproduction for academic, not-for profit purposes permitted provided this text is included.

- **Flexibility:** The limitation on the range size, encryption format and participants should be as little as possible.

Peng *et al* (Peng et al. 2006) analyse several related techniques including zero knowledge proof of partial knowledge by Cramer *et al* (Cramer, Damgård & Schoenmakers 1994), zero test by Peng *et al* (Peng, Boyd, Dawson & Lee 2004), a special proof and verification technique by Boudot (Boudot 2000) and other schemes (Bao 1998, Mao 1998, Brickell, Chaum, Damgård & van de Graaf 1987, Chan, Frankel & Tsiounis 1998, Peng, Boyd, Dawson & Lee 2005). They illustrate that their technique is more advanced than these previous techniques. Their method is simple: with the help of a second encryption system, a range test is reduced to a specialized zero test. The cryptographic primitive called specialized zero test in their paper is a special two party variant of a cryptographic tool called zero test in (Peng et al. 2004). A specialized zero test allows two parties, a ciphertext holder and a decryption key holder, to test whether at least one zero is encrypted in multiple ciphertexts held by the ciphertext holder where the decryption authority holds the private key. Their range test protocol, called precise range test, perfectly achieves correctness and flexibility. As their range test is reduced to a specialized zero test involving a small constant number (independent of the size of the range) of ciphertexts, it is efficient. However, its soundness and privacy are only achieved in the passive adversary model. Namely, the decryption authority is assumed not to deviate from the test protocol, which requires a trust on the decryption authority. This drawback greatly limits the application of their range test technique.

In this paper, cut-and-choose strategy is applied to optimise the range test protocol by Peng *et al* (Peng et al. 2006). In the optimised range test protocol, the tester does not need to trust the decryption authority. If the decryption authority is dishonest and deviates from the protocol, with an overwhelmingly large probability his invalid behaviour will be detected. Thus the optimised range test protocol is sound and private in the active adversary model. Although the cut-and-choose strategy leads to a trade-off between soundness and efficiency, the optimised range test protocol is still an efficient solution to range test.

In this paper, the following symbols are used.

- $\%$ denotes computation of remainder in a division.
- $|S|$ denotes the size of a set S .
- $\binom{a}{b}$ denotes the number of possible choices of b elements from a candidate elements.

The rest of the paper is organised as follows. In Section 2, the range test scheme by Peng *et al* (Peng

et al. 2006) is recalled and analysed. In Section 3, an optimisation of the range test scheme by Peng *et al* (Peng et al. 2006) is proposed. In Section 4, the new range test scheme is analysed. In Section 5, the new range test scheme is compared with the existing solutions.

2 The Range Test Scheme by Peng *et al*

Two additive homomorphic semantically-secure encryption systems (e.g. modified ElGamal encryption (Lee & Kim 2002)) are employed by Peng *et al* (Peng et al. 2006) in their range test where definition of additive homomorphic semantically-secure encryption is given as follows.

- An encryption algorithm with encryption function $E()$ is additive homomorphic if $E(m_1)E(m_2) = E(m_1 + m_2)$ for any messages m_1 and m_2 .
- An encryption algorithm is semantically-secure if given a ciphertext c and two messages m_1 and m_2 , such that $c = E(m_i)$ where $i = 1$ or 2 , there is no polynomial algorithm to find out i with a probability non-negligibly larger than 0.5 when the private key is unknown.

The tester holds a ciphertext in the first encryption system and cooperates with the authority, who holds the private key of the first encryption system. To implement the range test, a second encryption system is set up and its private key is held by the authority as well. The public keys of both encryption systems are public. The message spaces of the two encryption systems are Z_{p_1} and Z_{p_2} respectively. It is required that $p_2 \geq 3p_1$ and p_2 is a prime. The range involved in the test can be any Z_q with a condition $5q \leq p_1$. Peng *et al* (Peng et al. 2006) demonstrate that with the help of homomorphism of the employed encryption algorithm a range test in any range containing q consecutive integers can be reduced to a range test in interval range Z_q . As q can be very large, any interval range with practical size can be handled. Given a ciphertext c in the first encryption system, a tester A_1 has to test whether $D_1(c) < q$ with the help of A_2 , the decryption authority.

Peng *et al* (Peng et al. 2006) firstly propose a prototype protocol called basic range test implemented as follows where appropriate modulus dependent on the concrete encryption algorithm is used in every multiplication operation.

1. A_1 randomly chooses m_1 from Z_{p_1} . He calculates $c_1 = E_1(m_1)$ and sends $c_2 = c/c_1$ to A_2 .
2. A_2 calculates $m_2 = D_1(c_2)$, $c'_2 = E_2(m_2)$ and $e_2 = E_2(m_2 \% q)$. He then sends c'_2 and e_2 to A_1 .
3. A_1 calculates $c'_1 = E_2(m_1)$ and $e_1 = E_2(m_1 \% q)$. He then performs a specialized zero test:

$$\begin{aligned} ZM (A_1, A_2 \mid e_1 e_2 / (c'_1 c'_2), \\ e_1 e_2 / (c'_1 c'_2 E_2(q)), \\ e_1 e_2 / (c'_1 c'_2 E_2(p_1 \% q)), \\ e_1 e_2 / (c'_1 c'_2 E_2(p_1 \% q - q)), \\ e_1 e_2 / (c'_1 c'_2 E_2(p_1 \% q + q))) \end{aligned} \quad (1)$$

between A_1 , the ciphertexts holder, and A_2 , the decryption authority. A specialized zero test $ZM(c_1, c_2, \dots, c_n)$ checks whether at least one zero is encrypted in c_1, c_2, \dots, c_n and is implemented in Figure 1.

1. A_1 chooses $\pi()$, a permutation of $\{1, 2, \dots, n\}$, and random integers r_i from $Z_{p_2} \setminus \{0\}$ for $i = 1, 2, \dots, n$. Then he calculates $c'_i = c^{r_i}$ for $i = 1, 2, \dots, n$. He sends c'_1, c'_2, \dots, c'_n to A_2 .
2. A_2 calculates $d_i = D_2(c'_i)$ for $i = 1, 2, \dots, n$ one by one until one d_i is found to be zero or all the n ciphertexts are decrypted. He outputs TRUE iff a zero is found in his decryption.

Figure 1: Specialized zero test

A basic range test involving ciphertext c , tester A_1 and decryption authority A_2 is denoted as $BR (A_1, A_2 \mid c)$. Peng *et al* (Peng et al. 2006) prove that when the number of zeros encrypted in the tested integers is smaller than 2, specialized zero test does not reveal any information about the integers except whether there is a zero encrypted in them. As the employed encryption algorithms are semantically secure and among the five ciphertexts involved in (1) at most one of them can contain a zero, basic range test is private when it is strictly carried out. It is straightforward that it is correct. However its soundness is incomplete and it can only guarantee that $D_1(c) < 3q$. To solve this problem, Peng *et al* (Peng et al. 2006) propose their final solution, precise range test $PR (A_1, A_2 \mid c)$, described as follows.

1. A_1 communicates with A_2 to perform two basic range tests, $BR (A_1, A_2 \mid c)$ and $BR (A_1, A_2 \mid E_1(q-1)/c)$, in a random order.
2. A_2 finishes the two basic range tests and outputs:

$$PR (A_1, A_2 \mid c) = \begin{cases} \text{TRUE} & \text{if } BR (A_1, A_2 \mid c) = \text{TRUE} \text{ and} \\ & BR (A_1, A_2 \mid E_1(q-1)/c) = \text{TRUE} \\ \text{FALSE} & \text{otherwise} \end{cases}$$

Peng *et al* (Peng et al. 2006) prove that when A_2 does not deviate from the precise range test $PR (A_1, A_2 \mid c) = \text{TRUE}$ iff $D_1(c) < q$. They also prove that when A_2 does not deviate from the precise range test it is private and does not reveal any information about the secret message in c to any one except the test result. However, there is a drawback in the range test technique by Peng *et al* (Peng et al. 2006). As the decryption authority is assumed not to deviate from the precise range test, their test is only secure in the passive adversary model. In their test protocol, the decryption authority, A_2 must be trusted to be honest. Although A_1 as a tester must hope the protocol is strictly followed such that he can get the correct result, A_2 does not necessarily think in the same way. A_2 may cheat and lead the test protocol to a wrong result and thus their test protocol is not sound. Moreover, A_2 may replace his correct inputs with other inputs specially designed to obtain information about the secret message and thus compromise privacy of the test protocol.

3 Optimized Range Test

In this section, the precise range test by Peng *et al* (Peng et al. 2006) is optimized to be secure in the

1. A_1 chooses a security parameter t and randomly divides set $\{1, 2, \dots, 2t\}$ into four subsets S_1, S_2, S_3 and S_4 , such that $|S_1| + |S_2| = |S_3| + |S_4| = t$. He keeps this division secret.
2. A_1 randomly chooses m from Z_q , calculates $\hat{c} = E_1(m)$ and $E_1(0)$, a probabilistic encryption of zero. Then he repeats for $i = 1, 2, \dots, 2t$.
 - if $i \in S_1$, A_1 performs $VC_i = PR(A_1, A_2 | \hat{c})$ with A_2 ;
 - if $i \in S_2$, A_1 performs $VC_i = PR(A_1, A_2 | E_1(0)/\hat{c})$ with A_2 ;
 - if $i \in S_3$, A_1 performs $VC_i = PR(A_1, A_2 | c)$ with A_2 ;
 - if $i \in S_4$, A_1 performs $VC_i = PR(A_1, A_2 | E_1(0)/c)$ with A_2 .
3. A_1 recognises A_2 's honesty if and only if $VC_i = \text{TRUE}$ for $i \in S_1$, $VC_i = \text{FALSE}$ for $i \in S_2$, VC_i is identical for $i \in S_3$, VC_i is identical for $i \in S_4$ and $VC_i = \neg VC_j$ for $i \in S_3$ and $j \in S_4$. If A_2 is verified to be honest, A_1 accepts VC_i with $i \in S_3$ as the test result.

Figure 2: Optimized range test

active adversary model instead of only in the passive adversary model. In the passive adversary model, an adversary in a protocol may be curious and try to get information not supposed to be known by him, but he will not deviate from the protocol. It is also called honest-but-curious model. In the active adversary model, an adversary in a protocol not only may be curious but also may deviate from the protocol.

In the optimized range test A_1 employs a cut-and-choose mechanism to verify correctness of A_2 's operation. This cut-and-choose mechanism can also achieve complete privacy against A_2 . Multiple precise range tests of c are randomly mixed with multiple precise range tests of another random ciphertext. Only A_1 knows which precise range tests are performed on c , while A_2 cannot distinguish any test from other tests. If A_2 attempts to cause an incorrect result, with the help of the cut-and-choose mechanism A_1 can detect A_2 's cheating with an overwhelmingly large probability. The optimized range test protocol is described in Figure 2, which guarantees that the tester can always get the correct test result if he wants even in the active adversary model.

4 Analysis

Properties of the optimised range test is analysed in this section.

Theorem 1 *The probability that a cheating A_2 can pass the verification in the optimized range test is no more than $1/\binom{2t}{t}$.*

Proof: Let vc_i denote the result of the i^{th} precise range test when A_2 acts honestly. Let $CS = \{i \mid 1 \leq i \leq 2t, VC_i = vc_i\}$. No matter how A_2 cheats, his malicious behaviour can be classified into three cases:

$[CS] < t$, $t < [CS] < 2t$ or $[CS] = t$. In the following, these three cases are analysed respectively.

- If $[CS] < t$, $VC_i = \text{TRUE}$ for $i \in S_1$ and $VC_i = \text{FALSE}$ for $i \in S_2$ cannot be satisfied. So A_1 fails in the verification and A_2 is found cheating.
- If $t < [CS] < 2t$, either incorrect precise range test exists in VC_i for $i \in S_1 \cup S_2$ or both correct and incorrect precise range tests exist in VC_i for $i \in S_3 \cup S_4$. So A_1 fails in the verification and A_2 is found cheating.
- If $[CS] = t$, A_2 can pass the verification if and only if $CS = S_1 \cup S_2$. As A_1 keeps his division of the four sets secret and the employed encryption algorithms are semantically secure, A_2 cannot tell any difference between the multiple precise range tests in polynomial time. Moreover, S_1, S_2, S_3, S_4 are randomly chosen and $\{vc_1, vc_2, \dots, vc_{2t}\}$ are uniformly distributed in $\{\text{TRUE}, \text{FALSE}\}^{2t}$. So A_2 has no better method to find $S_1 \cup S_2$ other than random guess. Therefore, the probability that $CS = S_1 \cup S_2$ is $1/\binom{2t}{t}$.

Therefore, the only method for a cheating A_2 to pass the verification is to set $CS = S_1 \cup S_2$, the success probability of which is $1/\binom{2t}{t}$. \square

Theorem 1 indicates that if he wants the tester can always get the correct test result in the optimized precise range test with an overwhelmingly large probability even in the active adversary model.

Theorem 2 *The optimised range test is private.*

Proof: As the employed encryption algorithms are semantically secure and A_1 knows no private key, the only knowledge he gets in the optimized range test is the results of the $2t$ precise range tests if A_2 does not collude with him. As the results of the $2t$ precise range tests only contain the range test result of $D_1(c)$ and information about another message chosen by A_1 , A_1 's only knowledge about $D_1(c)$ is the test result. A_2 's knowledge from each precise range test is only the test result without A_1 's collusion. If A_1 does not collude with him, A_2 's knowledge transcript in each precise range test is independently distributed. So if A_1 does not collude with him, A_2 's knowledge about $D_1(c)$ in the optimized precise range test is the results of the $2t$ precise range tests, which are indistinguishable from each other. Therefore, A_2 's only knowledge about $D_1(c)$ is the test result. \square

The optimised range test protocol is flexible as it supports any additive homomorphic semantically-secure encryption, accepts ranges of the same magnitude as the size of the message space of the encryption algorithm and does not need any prover with knowledge of the encrypted message. Although the cut-and-choose mechanism reduces efficiency, cost of the optimized range test is still independent of the range size. As the cutting factor t (which is a small constant number like 20) is often much smaller than the range size, the optimized range test is still an efficient solution. So the optimized range test can satisfy all the desired properties of range test.

5 Comparison

The advantages of the new range test protocol over the existing related schemes in terms of the desired properties and efficiency are demonstrated in Table 1. In the comparison, cost of general and flexible range tests instead of more efficient range tests with special

encryption format for certain special application are listed. It is clearly demonstrated that the new scheme achieves all the desired properties of range test and is efficient.

The range test technique by Peng *et al* (Peng et al. 2006) only secure in the passive adversary model is optimised in this paper to be secure in the active adversary model. The new scheme achieves all the desired properties of range test and is efficient.

Acknowledgment

The research work is partially supported by NICT, Japan.

References

Bao, F. (1998), An efficient verifiable encryption scheme for encryption of discrete logarithms, in 'the Smart Card Research Conference, CARDIS'98', Vol. 1820 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 213–220.

Boudot, F. (2000), Efficient proofs that a committed number lies in an interval, in 'EUROCRYPT '00', Vol. 1807 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 431–444.

Brickell, E. F., Chaum, D., Damgård, I. B. & van de Graaf, J. (1987), Gradual and verifiable release of a secret, in 'Advances in Cryptology - Crypto '87', Vol. 293 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 156–166.

Chan, A., Frankel, Y. & Tsiounis, Y. (1998), Easy come - easy go divisible cash. updated version with corrections. Available as <http://www.ccs.neu.edu/home/yiannis/>.

Cramer, R., Damgård, I. B. & Schoenmakers, B. (1994), Proofs of partial knowledge and simplified design of witness hiding protocols, in 'CRYPTO '94', Vol. 839 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 174–187.

Lee, B. & Kim, K. (2002), Receipt-free electronic voting scheme with a tamper-resistant randomizer, in 'Information Security and Cryptology, ICISC 2002', Vol. 2587 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 389–406.

Mao, W. (1998), Guaranteed correct sharing of integer factorization with off-line share-holders, in 'Public Key Cryptography, 1st International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 1998', Vol. 1431 of *Lecture Notes in Computer Science*, Springer, Berlin, pp. 27–42.

Peng, K., Boyd, C., Dawson, E. & Lee, B. (2004), An efficient and verifiable solution to the millionaire problem, in 'ICISC 2004', Vol. 3506 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 315–330.

Peng, K., Boyd, C., Dawson, E. & Lee, B. (2005), Ciphertext comparison, a new solution to the millionaire problem, in 'ICICS 2005', Vol. 3783 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 84–96.

Peng, K., Boyd, C., Dawson, E. & Okamoto, E. (2006), A novel range test, in 'ACISP 2006', Vol. 4058 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 247–258.

Table 1: Property comparison

Scheme	Correctness & Soundness	Privacy	Large range	Prover with knowledge of the message	Format of the message	Cost
Range test based on (Cramer et al. 1994)	Yes	Yes	Yes	needed	any encryption or commitment	$O(q)$
Range test based on (Peng et al. 2004)	Yes	Yes	Yes	not needed	any additive homomorphic encryption	$O(q)$
Related technique in (Bao 1998, Mao 1998) (Brickell et al. 1987, Chan et al. 1998)	No	Yes	No	needed	commitment	$O(1)$
Related technique in (Boudot 2000)	asymptotical	Yes	No	needed	certain commitment	$O(1)$
Range test in (Peng et al. 2006)	in passive adversary model only	in passive adversary model only	Yes	not needed	any additive homomorphic encryption	$O(1)$
Optimized range test	Yes	Yes	Yes	not needed	any additive homomorphic encryption	$O(1)$