LUC vs KMOV

Bernadin Ibrahimpašić

Pedagogical Faculty, University of Bihać, Bosnia and Herzegovina

Będlewo, June, 10 - 12, 2010

RSA public – key cryptosystem

RSA public – key cryptosystem

- The most popular public–key cryptosystem in use today is the RSA.

RSA public – key cryptosystem

- The most popular public–key cryptosystem in use today is the RSA.
- Modulus n is the product of two distinct large primes p and q.

RSA public – key cryptosystem

- The most popular public–key cryptosystem in use today is the RSA.
- Modulus n is the product of two distinct large primes p and q.
- The public exponent e and the secret key d are related by

$$ed \equiv 1 \pmod{\varphi(n)}.$$

RSA public – key cryptosystem

- The most popular public–key cryptosystem in use today is the RSA.
- Modulus n is the product of two distinct large primes p and q.
- The public exponent e and the secret key d are related by

$$ed \equiv 1 \pmod{\varphi(n)}.$$

- The encryption and decryption algorithms are given by

$$C = M^e \bmod n \qquad \text{and} \qquad M = C^d \bmod n.$$

The security of the RSA

The security of the RSA

- The security of the RSA cryptosystem is based on the belief that the encryption function

$$e_K(M) = C = M^e \bmod n$$

is a one–way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext C.

The security of the RSA

- The security of the RSA cryptosystem is based on the belief that the encryption function

$$e_K(M) = C = M^e \bmod n$$

  is a one–way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext C.
- The trapdoor that allows Bob to decrypt a ciphertext is the knowledge of the factorization $n = pq$.

The security of the RSA

- The security of the RSA cryptosystem is based on the belief that the encryption function

$$e_K(M) = C = M^e \bmod n$$

  is a one–way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext C.
- The trapdoor that allows Bob to decrypt a ciphertext is the knowledge of the factorization $n = pq$.
- It is generally recommended that, to be on the safe side, one should choose each of p and q to be 512–bit primes.

The security of the RSA

- The security of the RSA cryptosystem is based on the belief that the encryption function

$$e_K(M) = C = M^e \bmod n$$

  is a one–way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext C.
- The trapdoor that allows Bob to decrypt a ciphertext is the knowledge of the factorization $n = pq$.
- It is generally recommended that, to be on the safe side, one should choose each of p and q to be 512–bit primes.
- I this case n will be a 1024–bit modulus.

The security of the RSA

- The security of the RSA cryptosystem is based on the belief that the encryption function

$$e_K(M) = C = M^e \bmod n$$

  is a one–way function, so it will be computationally infeasible for an opponent to decrypt a ciphertext C.
- The trapdoor that allows Bob to decrypt a ciphertext is the knowledge of the factorization $n = pq$.
- It is generally recommended that, to be on the safe side, one should choose each of p and q to be 512–bit primes.
- I this case n will be a 1024–bit modulus.
- Factoring a number of this size is well beyond the capability of the best current factoring algorithms.

LUC public – key cryptosystem

LUC public – key cryptosystem

- In 1993, Smith and Lennon described a new public–key cryptosystem based on a Lucas sequences.

LUC public – key cryptosystem

- In 1993, Smith and Lennon described a new public–key cryptosystem based on a Lucas sequences.
- It is developed in analogy with the RSA cryptosystem.

LUC public – key cryptosystem

- In 1993, Smith and Lennon described a new public–key cryptosystem based on a Lucas sequences.
- It is developed in analogy with the RSA cryptosystem.
- This cryptosystem is called LUC.

LUC public – key cryptosystem

- In 1993, Smith and Lennon described a new public–key cryptosystem based on a Lucas sequences.
- It is developed in analogy with the RSA cryptosystem.
- This cryptosystem is called LUC.
- The public key is (n, e), where n is the product of two large different primes p and q.

LUC public – key cryptosystem

- In 1993, Smith and Lennon described a new public–key cryptosystem based on a Lucas sequences.
- It is developed in analogy with the RSA cryptosystem.
- This cryptosystem is called LUC.
- The public key is (n, e), where n is the product of two large different primes p and q.
- The number e must be chosen so it is relatively prime to the product

$$(p-1)(q-1)(p+1)(q+1).$$

The Lucas sequences

The Lucas sequences

- Let a and b are nonzero integers and α and β the roots of the equation

$$x^2 - ax + b = 0.$$

The Lucas sequences

- Let a and b are nonzero integers and α and β the roots of the equation

$$x^2 - ax + b = 0.$$

- The Lucas sequences

$$(U_n) \qquad \text{and} \qquad (V_n), \quad (n \geq 0)$$

are given by

The Lucas sequences

- Let a and b are nonzero integers and α and β the roots of the equation

$$x^2 - ax + b = 0.$$

- The Lucas sequences

$$(U_n) \qquad \text{and} \qquad (V_n), \quad (n \geq 0)$$

are given by

$$U_n \quad = \quad aU_{n-1} - bU_{n-2}, \quad U_0 = 0, \quad U_1 = 1,$$

The Lucas sequences

- Let a and b are nonzero integers and α and β the roots of the equation

$$x^2 - ax + b = 0.$$

- The Lucas sequences

$$(U_n) \qquad \text{and} \qquad (V_n), \quad (n \geq 0)$$

are given by

$$\begin{aligned} U_n &= aU_{n-1} - bU_{n-2}, \quad U_0 = 0, \quad U_1 = 1, \\ V_n &= aV_{n-1} - bV_{n-2}, \quad V_0 = 2, \quad V_1 = a. \end{aligned}$$

LUC – encription and decription

LUC – encription and decription

- Let M be a message which is less than n and relatively prime to n.

LUC – encription and decription

- Let M be a message which is less than n and relatively prime to n.
- We obtain the ciphertext C by

$$C = V_e(M, 1) \mod n.$$

LUC – encription and decription

- Let M be a message which is less than n and relatively prime to n.
- We obtain the ciphertext C by

$$C = V_e(M, 1) \mod n.$$

- The public number e and the secret number d are related by

$$ed \equiv 1 \pmod{S(n)},$$

where

$$S(n) = \operatorname{lcm}(p \pm 1, q \pm 1).$$

LUC – encription and decription

- Let M be a message which is less than n and relatively prime to n.
- We obtain the ciphertext C by

$$C = V_e(M, 1) \mod n.$$

- The public number e and the secret number d are related by

$$ed \equiv 1 \pmod{S(n)},$$

where

$$S(n) = \operatorname{lcm}(p \pm 1, q \pm 1).$$

- The decription process is then the same as encryption, with e replaced by d, and we have

$$M = V_d(C, 1) \mod n.$$

KMOV public – key cryptosystem

KMOV public – key cryptosystem

- In 1991, Koyama, Maurer, Okamoto and Vanstone proposed public key cryptosystem which is an elliptic curve based analogue to RSA.

KMOV public – key cryptosystem

- In 1991, Koyama, Maurer, Okamoto and Vanstone proposed public key cryptosystem which is an elliptic curve based analogue to RSA.
- Their cryptosystem is based on the difficulty of factoring large numbers.

KMOV public – key cryptosystem

- In 1991, Koyama, Maurer, Okamoto and Vanstone proposed public key cryptosystem which is an elliptic curve based analogue to RSA.
- Their cryptosystem is based on the difficulty of factoring large numbers.
- The authors propose using the elliptic curve $E_n(0, b)$ with equation

$$y^2 = x^3 + b \bmod n.$$

KMOV public – key cryptosystem

- In 1991, Koyama, Maurer, Okamoto and Vanstone proposed public key cryptosystem which is an elliptic curve based analogue to RSA.
- Their cryptosystem is based on the difficulty of factoring large numbers.
- The authors propose using the elliptic curve $E_n(0, b)$ with equation

$$y^2 = x^3 + b \bmod n.$$

- Modulus n is the product of two large different primes p and q, are both congruent to 2 mod 3.

KMOV public – key cryptosystem

- In 1991, Koyama, Maurer, Okamoto and Vanstone proposed public key cryptosystem which is an elliptic curve based analogue to RSA.
- Their cryptosystem is based on the difficulty of factoring large numbers.
- The authors propose using the elliptic curve $E_n(0, b)$ with equation

$$y^2 = x^3 + b \bmod n.$$

- Modulus n is the product of two large different primes p and q, are both congruent to 2 mod 3.
- The public number e and the secret number d are related by

$$ed \equiv 1 \quad \operatorname{lcm}(p+1, q+1).$$

KMOV – encription and decription

KMOV – encription and decription

- Alice want to send a message M to Bob.

KMOV – encription and decription

- Alice want to send a message M to Bob.
- She represents her message as a pair of integers (m_1, m_2) (mod n).

KMOV – encription and decription

- Alice want to send a message M to Bob.
- She represents her message as a pair of integers (m_1, m_2) (mod n).
- She regards (m_1, m_2) as a point M on the elliptic curve $E_n(0, b)$.

KMOV – encription and decription

- Alice want to send a message M to Bob.
- She represents her message as a pair of integers (m_1, m_2) (mod n).
- She regards (m_1, m_2) as a point M on the elliptic curve $E_n(0, b)$.
- Alice adds M to itself e times on E_n to obtain

$$C = (c_1, c_2) = eM.$$

KMOV – encription and decription

- Alice want to send a message M to Bob.
- She represents her message as a pair of integers (m_1, m_2) (mod n).
- She regards (m_1, m_2) as a point M on the elliptic curve $E_n(0, b)$.
- Alice adds M to itself e times on E_n to obtain

$$C = (c_1, c_2) = eM.$$

- She sends C to Bob.

KMOV – encription and decription

- Alice want to send a message M to Bob.
- She represents her message as a pair of integers (m_1, m_2) (mod n).
- She regards (m_1, m_2) as a point M on the elliptic curve $E_n(0, b)$.
- Alice adds M to itself e times on E_n to obtain

$$C = (c_1, c_2) = eM.$$

- She sends C to Bob.
- Bob computes $M = dC$ on E_n to obtain M.

Wiener

Wiener

- In 1990 Wiener described an attack on typical RSA with small secret exponent.

Wiener

- In 1990 Wiener described an attack on typical RSA with small secret exponent.
- He showed that if

$$d < n^{0.25},$$

then d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n.

Wiener

- In 1990 Wiener described an attack on typical RSA with small secret exponent.
- He showed that if

$$d < n^{0.25},$$

then d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n.

- His result is based on the classical Legendre's theorem on Diophantine approximations of the form

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

Verheul and van Tilborg

Verheul and van Tilborg

- In 1997, Verheul and van Tilborg extended the boundary of the Wiener attack on RSA.

Verheul and van Tilborg

- In 1997, Verheul and van Tilborg extended the boundary of the Wiener attack on RSA.
- They propose a technique to raise the security Wiener's boundary of $n^{0.25}$ with exhaustive-searching for $2t + 8$ bits, where

$$t = \log_2 d - \log_2 n^{0.25}.$$

Verheul and van Tilborg

- In 1997, Verheul and van Tilborg extended the boundary of the Wiener attack on RSA.
- They propose a technique to raise the security Wiener's boundary of $n^{0.25}$ with exhaustive-searching for $2t + 8$ bits, where

$$t = \log_2 d - \log_2 n^{0.25}.$$

- The candidates for the secret key d are of the form

$$d = rq_{m+1} + sq_m,$$

for some nonnegative integers r and s.

Dujella

Dujella

- In 2004, Dujella described a new variant of the Wiener attack on RSA.

Dujella

- In 2004, Dujella described a new variant of the Wiener attack on RSA.
- His attack is a modification of the Verheul and van Tilborg variant, and it is based on the Worley result on Diophantine approximations of the form

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

where c is a positive real number.

Dujella

- In 2004, Dujella described a new variant of the Wiener attack on RSA.
- His attack is a modification of the Verheul and van Tilborg variant, and it is based on the Worley result on Diophantine approximations of the form

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

where c is a positive real number.

- The candidates for the secret exponent d are of the form

$$d = rq_{m+1} \pm sq_m,$$

for some nonnegative integers r and s such that $rs < 2c$.

Our atack on LUC and KMOV public–key cryptosystems

Our atack on LUC and KMOV public–key cryptosystems

- In 1995, Pinch extended the Wiener attack to LUC and KMOV cryptosystems.

Our atack on LUC and KMOV public–key cryptosystems

- In 1995, Pinch extended the Wiener attack to LUC and KMOV cryptosystems.
- Pinch showed that both cryptosystems with 1024–bit modulus n are insecure for 256–bit private key d.

Our atack on LUC and KMOV public–key cryptosystems

- In 1995, Pinch extended the Wiener attack to LUC and KMOV cryptosystems.
- Pinch showed that both cryptosystems with 1024–bit modulus n are insecure for 256–bit private key d.
- We extend the Dujella variant of the Wiener attack to LUC and KMOV cryptosystems.

Our atack on LUC and KMOV public–key cryptosystems

- In 1995, Pinch extended the Wiener attack to LUC and KMOV cryptosystems.
- Pinch showed that both cryptosystems with 1024–bit modulus n are insecure for 256–bit private key d.
- We extend the Dujella variant of the Wiener attack to LUC and KMOV cryptosystems.
- We describe an algorithm for finding secret key d, where

$$d = rq_{m+1} \pm sq_m,$$

for some nonnegative integers r and s.

Our atack on LUC and KMOV public–key cryptosystems

Our atack on LUC and KMOV public–key cryptosystems

- Using results on connection between continued fractions and rational approximations of the form

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

for a positive integer c, from Dujella and Ibrahimpašić and results on Diophantine approximations from Dujella and Worley, we derive bounds for r and s.

Our atack on LUC and KMOV public–key cryptosystems

- Using results on connection between continued fractions and rational approximations of the form

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

for a positive integer c, from Dujella and Ibrahimpašić and results on Diophantine approximations from Dujella and Worley, we derive bounds for r and s.

- We have implemented our attack in the computer algebra system PARI/GP (on a 3.0GHz – Pentium under Windows XP).

Our atack on LUC and KMOV public–key cryptosystems

Our atack on LUC and KMOV public–key cryptosystems

- It works efficiently for

$$D \leq 2^{14},$$

such that

$$d < Dn^{0.25}.$$

Our atack on LUC and KMOV public–key cryptosystems

- It works efficiently for

$$D \leq 2^{14},$$

such that

$$d < Dn^{0.25}.$$

- More precisely, an implementation of this attack needs in average around

Our atack on LUC and KMOV public–key cryptosystems

- It works efficiently for

$$D \leq 2^{14},$$

such that

$$d < Dn^{0.25}.$$

- More precisely, an implementation of this attack needs in average around
  - One hour for $D \leq 2^{13}$, and

Our atack on LUC and KMOV public–key cryptosystems

- It works efficiently for

$$D \leq 2^{14},$$

such that

$$d < Dn^{0.25}.$$

- More precisely, an implementation of this attack needs in average around
  - One hour for $D \leq 2^{13}$, and
  - Around 5 hours for $D \leq 2^{14}$.

Our atack on LUC and KMOV public–key cryptosystems

- It works efficiently for

$$D \leq 2^{14},$$

such that

$$d < Dn^{0.25}.$$

- More precisely, an implementation of this attack needs in average around
  - One hour for $D \leq 2^{13}$, and
  - Around 5 hours for $D \leq 2^{14}$.
- Thus, we conclude that our attack shows that LUC and KMOV cryptosystems, with 1024–modulus n, are insecure for 270–bit secret key d.

References

1. B. Ibrahimpašić, *Comparing the security of LUC and KMOV public–key cryptosystems*, NATO Advanced Study Institute on Information Security and Related Combinatorics, Opatija, 2010
2. A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29**(2004)
3. A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, Ann. Math. Inform. **35**(2008)
4. B. Ibrahimpašić, *Cryptanalysis of KMOV cryptosystem with short secret exponent*, Proceedings of the 19^{th} Central European Conference on Information and Intelligent Systems, 2008
5. B. Ibrahimpašić, *Cryptanalysis of LUC cryptosystem with short secret exponent*, Book of the abstracts of 8^{th} Central European Conference on Cryptography, Graz, 2008
6. B. Ibrahimpašić, *Cryptanalysis of LUC cryptosystem with short secret exponent*, Math. Commun. **14–1**(2009)
7. B. Ibrahimpašić, *Security of KMOV and LUC cryptosystem*, Proceedings of the 7^{th} International Scientific Conference RIM2009, Cairo, 2009

References

8. K. Koyama, U. M. Maurer, T. Okamoto, S. A. Vanstone: New public–key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, Advances in Cryptology - Crypto '91, Lecture Notes in Computer Science, vol. 576, Springer–Verlag, 1991, pp. 252–266.
9. R. G. E. Pinch, *Extending the Wiener attack to RSA–type cryptosystems*, Electronics Letters **31**(1995), 1736–1738.
10. R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public–key cryptosystems*, Communications of the ACM **21**(1978), 120–126.
11. P. J. Smith, G. J. J. Lennon, *LUC: a new public–key cryptosystem*, Ninth IFIP Symposium on Computer Science Security, Elseviver Science Publishers, (1993), 103–117.
12. E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8**(1997), 425–435.
13. M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.
14. R. T. Worley, *Estimating* $|\alpha - p/q|$, Austral. Math. Soc. Ser. A **31** (1981), 202–206.

THANK YOU FOR YOUR ATTENTION