格構造優化技術及在公開金鑰密碼分析中的應用

盧堯[1,2]，林東岱[1]
[1]中國科學院信息工程研究所 信息安全國家重點實驗室
[2]中國科學院大學
{luyao, ddlin}@iie.ac.cn

摘要

基於格的密碼分析技術（簡稱格分析技術）通常是利用格基約化演算法來尋找密碼系統內參數向量之間的短的線性關係，借此來對恢復金鑰資訊的分析技術。利用格分析技術分析已有的密碼演算法，特別是基於大整數分解和離散對數困難問題的公開金鑰密碼演算法，能夠更深入的挖掘原有密碼系統的代數結構，發現之前未能發現的金鑰資訊，是密碼分析中一個強有力的工具。本文主要對格分析技術及其在公開金鑰密碼分析中的應用進展做一個綜述性的介紹，希望對此主題感興趣的讀者有所啟發。

關鍵詞：格分析技術，RSA，DSA，基於背包的密碼系統

壹、前言

密碼學是門古老的學科，它的起源可追溯到古羅馬和希臘時期。一般來說，密碼學可分成兩個分支：一類是密碼設計，一類是密碼分析。密碼設計主要任務是根據實際環境，設計新的密碼方案；而密碼分析則是發現密碼演算法中的弱點，嘗試去攻破。這兩類密碼學的分支是相互促進，相輔相成的，一方面，新的密碼方案產生了許多新的問題去研究，另一方面，新的分析技術的產生導致新的密碼演算法的發現。在最初的幾個世紀裡，密碼技術一直只應用於軍事領域，但在最近幾十年，隨著資訊化的不斷深入，密碼技術的應用環境發生了巨大的變化，密碼已經滲透到人們生活的方方面面，特別是電腦網路廣泛使用的今天，我們每一次查看電子郵件，或用蜂窩電話打個電話，或者通過互聯網進行一次購物，我們都要依靠密碼技術來保護我們資料的完整性、真實性和隱私性。

密碼學最根本的目標是加密一段消息使得只有擁有正確金鑰的接收者才能正確的解密。為了安全的通信，這就需要消息的發送者和接受者共同分享一個金鑰，這種雙方利用相同的金鑰進行加解密資訊的密碼被稱為對稱密碼，但在複雜的網路環境中，它的應用大大受限。1976 年，Diffie 和 Hellman 的開創性工作[16]提出了公開金鑰密碼的思想，公開金鑰密碼與之前使用的單一工作階段金鑰的對稱密碼的最大不同在於所有使用公開金鑰密碼演算法的使用者都擁有一對金鑰：一個公開，用於加密，簡稱公開金鑰；另一個為用戶私有，用於解密，簡稱私密金鑰。這裡可以看到公開金鑰和私密金鑰是不同的，所以公開金鑰密碼又稱非對稱密碼，其對於通信環境的安全性要求相對比較弱，更適用於目前複雜的網路環境中。

1978 年，Rivest，Shamir 和 Adleman 設計出第一個公開金鑰密碼演算法—RSA，該演算法的安全性依賴於大整數分解難題，演算法本身易於理解和實現，因此在資訊安全領域得到了廣泛的應用。國際上一些標準化組織 ISO，ITU，SWIFT 等都已接受 RSA 密碼體制作為標準，在 Internet 中，電子郵件是最常用的一種網路服務，廣泛採用的 PGP(Pretty Good Privacy)技術就是用 RSA 演算法作為傳送工作階段金鑰和數位簽章的標準演算法來保證電子郵件中的機密性和身份認證。因此，如何衡量 RSA 演算法及基於其構造的密碼方案的安全性一直是公開金鑰密碼最為重要的問題之一。

從 RSA 演算法提出到現在的三十多年時間裡，RSA 是被研究的最為廣泛、深入和徹底的公開金鑰密碼演算法，經歷了各種攻擊的考驗。截至目前，在非量子計算模型假設下，還沒有任何攻擊演算法能夠威脅 RSA 演算法本身的安全性，因此，關於 RSA 演算法的安全性分析工作也一直是密碼學界研究的難點之一。其中，1996 年，Coppersmith[12]提出基於格基約化的分析技術來求解模方程和整係數方程小根的演算法，改變了之前近二十年 RSA 研究結果很少的尷尬局面，對於 RSA 密碼演算法的安全性分析起了巨大的推動作用。正是基於此，格分析技術引起了密碼學者的廣泛關注，目前已成為公開金鑰密碼學研究的熱點之一。

同時，正如前面所說，新的密碼分析技術帶動新的密碼演算法的發現，密碼學者研究發現，從演算法複雜性的角度研究格理論，其具備一些獨特的性質。1996 年，Ajtai 在文獻中[2]開創性的證明了某些著名的個問題在平均情況下的複雜性和最壞情況下的複雜性之間存在著等價關係，由此結論，Ajtai 和 Dwork 在 1997[3]年設計了第一個基於格的公開金鑰方案-AD 方案，隨後，出現了很多基於格上困難問題的公開金鑰密碼演算法，包括著名的抗碰撞的雜湊函數的 GGH[22]演算法、已被寫入國際標準的 NTRU[26]加密演算法等；此外，由於格是一種線性結構，其上的運算都是線性運算，因此格方案比 RSA，ECC 等傳統加密方案具有更快的運算速度。近年來，針對于不同的應用環境，許多基於格理論的密碼方案被提出，其中影響最大的是 2009 年 Gentry[22]利用理想格提出了第一個全同態加密方案，解決了困擾密碼學界近 20 年的難題。

綜上所述，格分析技術的發展，不僅使得人們對於經典的密碼體制（如 RSA）的安全性有了更清楚的認識，而且帶動了新的基於格的密碼方案的發展。因此，對格分析技術的研究，不僅在學術上有很高的研究價值，而且在應用領域上具有廣泛的前景。

貳、格分技術

格分析技術通常是利用格基約化演算法來尋找密碼系統內參數向量之間的短的線性關係，借此來恢復金鑰資訊的分析技術。粗略的講，格分析技術可以分為兩類：一類是直接的格分析技術，顧名思義，它一般是將攻擊密碼系統直接歸約到求解格中的一類困難問題，如 SVP 問題；一類是 Coppersmith 方法，它是利用格基約化技術，將破解密碼系統歸約到求解方程或方程組小根問題。

直接的格分析技術主要利用密碼系統參數之間的關係，尋找它們之間短的係數的線性關係，這些係數一般是屬於整數或模數環上的，從而發現金鑰的某些資訊。這種直接的格分析技術是根據不同的密碼系統，採取不同的策略，因此很難給出一個固定的求解模式，我們將在下節的應用中給出它對一些經典的密碼系統的分析結果。

Coppersmith 技術是求解方程或方程組小根的一類技術，一些密碼系統的金鑰恢復最終可歸約到求解方程或方程組的小根問題上。這種技術在 1996 年由 Coppersmith 提出，演算法背後的主要思想是將方程的係數向量按某種方式構造一個格，然後利用格基約化演算法，尋找到長度短的向量，期望短向量對應的方程的根在整數方程上也成立。Coppersmith 針對高次單變元模方程提出了一類解法，1997 年，Howgrave-Graham[27]重新解釋了 Coppersmith 的方法，他的方法簡明易懂，之後許多的學者[55]都沿用了他的工作。

在文獻[10]中，Coppersmith 還提出了一類二次二變元的整數方程求解演算法，但是演算法複雜難懂，2007 年，Coron 在文獻[12]中給出了一類簡化演算法，與 Howgrave-Graham 方法類似，將整數方程轉化到模方程中進行處理，且和 Coppersmith 方法具有相同的漸進效率。此外，在文獻[32]中，作者針對一般形式的模方程和整數方程給出了一個一般性的求解小根的演算法。

說到格分析技術，不得不說到格基約化演算法，它是用來求解格中短向量的方法，是整個格分析演算法裡非常重要的一環。在實際中，我們經常用到的是由 A.K.Lentra，H.W.Lenstra，和 L.Lovasz 在 1982 年提出的 LLL 演算法[39]。該演算法在多項式時間內，輸出近似因數為$((1+\epsilon)\sqrt{4/3})^{(n-1)/2}$的短向量，這裡$\epsilon$是一個正的常數。LLL 演算法的提出不僅對公開金鑰密碼演算法的分析起到了很大的推動作用，而且在計算代數、計算數論等領域也有廣泛的應用。

參、格分析技術在公開金鑰密碼中的應用

3.1 背包密碼體制安全性分析

背包密碼體制是由 Merkel-Hellman 提出的，它是基於子集和困難問題構造的一類公開金鑰密碼方案。子集和問題是指，給定正整數$a_1,\ldots,a_n$和s滿足線性方程

$$x_1a_1+\cdots+x_na_n=s$$

求解未知量$x_1,\ldots,x_n\in\{0,1\}$。格分析技術來攻擊背包問題的主要思想是將子集和問題的求解轉化到尋找格上的某個短向量，這裡用到了我們上節提到的直接的格分析技術。

1982 年，Shamir[50]首先提出破解基本的 Merkel-Hellman 背包密碼體制的多項式時間演算法。其主要思想是即利用多項式時間內求解關於固定數量變元的整數規劃解決背

包密碼演算法中的問題。隨後，1985 年，Lagarias 和 Odlyzko[36]構造了一類格，利用 LLL 演算法求解格的短向量，從而破解了密度小於 0.646 的背包體制。之後，Coster，Lamacchia 和 Odlyzko[14]通過構造不同的格，將結果改進到 0.9408。之前文獻的結果都是基於l_2範數的。最近，Hu，Pan 和 Zhang[30]推廣到l_p $(p \geq 3)$範數上。

3.2 RSA 安全性分析

本小節我們介紹利用格分析技術來攻擊 RSA 的相關研究工作，這方面開創性的工作是由 Coppersmith[10]提出的求解模方程或整數方程小根的格分析技術。

眾所周知，RSA 演算法的安全性是建立在大整數分解問題的困難性上。如果能分解大整數，那麼很容易攻破 RSA，但是存在一個多項式時間演算法能攻破 RSA，是否能利用這個演算法在多項式時間內分解大整數呢？密碼學者在這方面做了很多研究工作[1,8,38]，但至今這個問題沒有定論，是密碼學中一個著名的公開問題。目前已知的演算法都是來通過恢復金鑰d來破解 RSA，1975 年，Miller[46]的結果表明分解大整數和計算d存在著概率多項式時間歸約。利用格基約化技術，May 和 Coron[13]給出了一個確定的多項式時間演算法，即給定(N, e, d)，他們的演算法可在確定多項式時間內分解整數N。可惜的是，他們的演算法當$ed < N^2$時有效，當$ed > N^2$，至今仍是一個公開問題。

目前最好的分解大整數的演算法仍是亞指數時間的，但當已知某個素因數的連續比特資訊時，利用格分析技術，我們可以有效的分解大整數。這方面有代表性的研究工作是：已知素因數的某些比特來分解大整數（Factoring with Known Bits Problem）[7,10,42]，隱式分解大整數（Implicit Factorization Problem）[20,45]。

由於 RSA 涉及到很多的模乘運算，因此速度是它的一個很大瓶頸，在實際中，我們常常採用一些長度短的d，這樣能大大加速 RSA 演算法的效率，但這樣做是否是安全的呢？1990 年，Wiener 利用連分式技術，當$d < N^{0.25}$時，有效的分解了大整數N。隨後，Boneh 和 Durfee[5]利用格分析技術將 Wiener 的結果改進到$d < N^{0.284}$，緊接著，他們觀察到可以利用格中的一類子格可將結果進一步改進至$d < N^{0.292}$。其中，他們所用子格組成的矩陣並不是一個三角矩陣，因此計算它的行列式十分的複雜，2010 年，Herrmann 和 May[25]利用一種名為 Unravelled Linearization 的格優化技術給出了一個簡潔的證明，其後，Kunihiro 等人[35]綜合 May[43]和 Herrmann-May[25]的技術，做了更深入的研究。但是，很可惜，目前最好的結果仍是$d < N^{0.292}$，不少學者認為這應該是格分析技術所能攻擊的極限。

側通道攻擊可以獲得金鑰d的部分比特資訊，研究如何利用這些洩漏的比特資訊有效的破解 RSA 演算法是具有實際應用價值的問題。這類問題被稱為洩漏部分金鑰攻擊，關於這類問題的研究，國外學者已經得到了不少的結果：1998 年，Boneh 等人[6]研究了金鑰d洩漏某些高位或低位元比特資訊對於 RSA 演算法安全性的影響，他們的攻擊演算法僅當加密指數e較小時是有效的，隨後，在 2003 年，Blomer 和 May[31]給出了幾種當加

密指數e較大情形下的有效攻擊。緊接著，2005 年，Ernst 等人[18]進一步將攻擊擴展到$e \approx N$的情況。

為了抵抗上述的攻擊或加快 RSA 加解密速度，我們常常會在實際中，針對不同的應用場景，採用不同的變種 RSA 演算法，這裡我們給出格基約化演算法對四種 RSA 變種演算法的安全性分析：CRT-RSA，Multi-Prime RSA，Multi-Power RSA 和 Common Prime RSA。

1) CRT-RSA：首先由 Quisquater 和 Couvreur 提出，是目前實際中的 RSA 的標準。利用格基約化技術對它的分析主要包括[4,33,42]。
2) Multi-Power RSA：這種變種 RSA 演算法由 Takagi 首次提出，目前已成為國際標準。利用格基約化技術對它的分析主要包括[7,34]。
3) Common Prime RSA：為了抵抗小解密指數對 RSA 的攻擊，我們在選取素因數的時候，會選擇$\gcd(p-1, q-1) = g$，其中g是一個較大的素數，這就是 Common Prime RSA。利用格基約化技術對它的分析主要包括[32]。

此外，格分析還對一些其他變種的 RSA 演算法具有很好的分析結果，具體的內容見文獻[17]。

格分析技術還對一些與 RSA 相關的困難問題假設有著很好的分析，如對Φ-hiding 假設的分析[23]。

3.3 DSA/ECDSA 簽名演算法安全性分析

DSA（Digital Signature Algorithm）是美國國家標準與技術研究院（NIST）公佈的簽名演算法的標準，它作為 ElGamal 和 Schnorr 簽名演算法的變種，其安全性是基於有限域上的離散對數困難問題。而 ECDSA 是 DSA 的橢圓曲線版本，安全性是基於橢圓曲線上的離散對數的困難問題。

這兩個簽名演算法每運行一次，需要一個亂數 nonce，這個亂數一是用來生成一個離散對數問題，二是和密碼系統的公私密金鑰參數生成簽名的一部分。因 nonce 是和私密金鑰綁定的，如果知道了 nonce，那麼我們就可以恢復私密金鑰。格分析技術對簽名演算法的分析主要是利用 nonce和公私密金鑰參數一起生成的代數等式，利用多個簽名，從而恢復出私密金鑰。

2001 年，Howgrave-Graham 和 Smart[29]分析了在 DSA 部分 nonce 已知的情況下，給出了一個基於格的啟發式攻擊。後來，Nguyen 和 Shparlinski[48]改進了這個結果，給出了一個可證明的多項式時間攻擊。實驗結果可在已知 nonce 的低位 3 比特，100 個簽名的情況下恢復金鑰。2013 年，Liu 和 Nguyen[40]利用裁剪枚舉求解 BDD 問題進一步改進了這個結果，將 nonce 洩露的比特數降到 2 比特。

此外，還有一些硬體實現上對 DSA 和 ECDSA 的物理攻擊，其中包括有當 nonce 比特形式為$k = y|y|x$時的恢復金鑰攻擊[37]，亂數發生器生成的 nonce 共用高位或低位元比

特資訊的金鑰恢復攻擊[19]，和利用 Bleichenbacher 技術來攻擊 ECDSA[15]等。

3.4、其他密碼體制的分析

格基約化技術還可以用來分析基於格的密碼方案，如 1999 年 Nguyen[47]成功破解了 GGH 密碼方案給出的 5 個挑戰密文其中的 4 個。

目前著名的 NTRU 加密方案的大部分分析結果也是由格基約化技術得到的[11,28]。NTRU 加密方案是由 Hoffstein，Pipher 和 Silverman[26]在 1998 年提出的，該方案的安全性可歸約到求解格中最短向量或最近向量問題的困難性上。相比於 RSA，ECC，NTRU 加解密速度更快，被認為是下一代公開金鑰密碼方案的有力競爭者。且 2008 年 IEEE 標準 1363.1 制定了基於格的密碼方案，主要就是 NTRU 加密方案標準。

此外，格還可以用來分析背包問題和格混合的公開金鑰密碼方案，如 1999 年，Cai 和 Cusick[9]通過在 Ajtai-Dwork 方案混入一個背包結構提出了一個公開金鑰方案，後來，Pan 等人[49]針對該方案利用一個反覆運算演算法給出了一個唯密文攻擊。

肆、結論

格分析技術是密碼分析中主流的一類分析技術，在本文中，我們對其技術本身以及在公開金鑰密碼中的應用的發展做了一個簡要的回顧，可以看到，格分析技術針對目前已有的大部分公開金鑰密碼演算法，都有很好的分析結果。

參考文獻

[1] D. Aggarwal and U. Maurer, “Breaking RSA generically is equivalent to factoring,” *In Advances in Cryptology-EUROCRYPT 2009*. Springer, 2009, pp. 36–53.

[2] M. Ajtai, “Generating hard instances of lattice problems,” In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (1996), ACM, pp. 99–108.

[3] M. Ajtai and C. Dwork., “A public-key cryptosystem with worst-case/average-case equivalence,” In Proceedings of the twenty-ninth annual ACM symposium on Theory of computing (1997), ACM, pp. 284–293.

[4] D. Bleichenbacher and A. May, “New attacks on RSA with small secret CRT-exponents,” Public Key Cryptography–PKC 2006 (2006), 1–13.

[5] D. Boneh and G. Durfee, “Cryptanalysis of RSA with private key less than N0.292 ,” IEEE Transactions on Information Theory 46, 4 (2000), 1339–1349.

[6] D. Boneh, G. Durfee, and Y. Frankel, "An attack on RSA given a small fraction of the private key bits," In Advances in Cryptology–ASIACRYPT'98 (1998), Springer, pp. 25–34.

[7] D. Boneh, G. Durfee, and N. Howgrave-Graham, "Factoring N =prq for large r," In Advances in Cryptology–CRYPTO'99 (1999), Springer, pp. 787–787.

[8] D. Boneh. and R. Venkatesan, "Breaking RSA may not be equivalent to factoring," In Advances in Cryptology-EUROCRYPT'98. Springer, 1998,pp. 59–71.

[9] J. Cai. and T. Cusick, "A lattice-based public-key cryptosystem," In Selected Areas in Cryptography (1999), Springer, pp. 219–233.

[10] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," Journal of Cryptology 10, 4 (1997), 233–260.

[11] D. Coppersmith. and A. Shamir, "Lattice attacks on NTRU," In Advances in Cryptology-EUROCRYPT'97 (1997), Springer, pp. 52–61.

[12] J. Coron, "Finding small roots of bivariate integer polynomial equations: A direct approach," In Advances in Cryptology–CRYPTO 2008 (2008), Springer-Verlag, pp. 379–394.

[13] J. Coron. and A. May, "Deterministic polynomial-time equivalence of computing the RSA secret key and factoring," Journal of Cryptology 20,1 (2007), 39–50.

[14] M. Coster, B. LaMacchia, A. Odlyzko and C. Schnorr, "An improved low-density subset sum algorithm," In Advances in Cryptology-EUROCRYPT'91 (1991), Springer, pp. 54–67.

[15] E. D. Mulder, M. Hutter, M. Marson and P. Pearson, "Using Bleichenbacher's solution to the hidden number problem to attack nonce leaks in 384-bit ECDSA: extended version," Journal of Cryptographic Engineering 4, 1 (2014), 33–45.

[16] W. Diffie. and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory 22, 6 (1976), 644–654.

[17] G. Durfee. and P. Nguyen, "Cryptanalysis of the RSA schemes with short secret exponent from Asiacrypt'99," In Advances in Cryptology-ASIACRYPT 2000 (2000), 14–29.

[18] M. Ernst, E. Jochemsz, A. May. and B. D. Weger, "Partial key exposure attacks on RSA up to full size exponents," In Advances in Cryptology–EUROCRYPT 2005 (2005), 555–555.

[19] J. Faugère, C. Goyet. and G. Renault, "Attacking (EC) DSA given only an implicit hint," In Selected Areas in Cryptography (2013), Springer, pp. 252–274.

[20] J. Faugère, R. Marinier. and G. Renault, "Implicit factoring with shared most significant and middle bits," Public Key Cryptography–PKC 2010 (2010), 70–87.

[21] C. Gentry, "Fully homomorphic encryption using ideal lattices," In STOC (2009), vol. 9, pp. 169–178.

[22] O. Goldreich, S. Goldwasser. and S. Halevi, "Public-key cryptosystems from lattice reduction problems," In Advances in Cryptology-CRYPTO'97. Springer, 1997, pp. 112–131.

[23] M. Herrmann, "Improved cryptanalysis of the multi-prime φ-hiding assumption," Progress in Cryptology–AFRICACRYPT 2011 (2011), 92–99.

[24] M. Herrmann and A. May, "Solving linear equations modulo divisors: On factoring given any bits," In Advances in Cryptology-ASIACRYPT 2008(2008), 406–424.

[25] M. Herrmann and A. May, "Maximizing small root bounds by linearization and applications to small secret exponent RSA," Public Key Cryptography–PKC 2010 (2010), 53–69.

[26] J. Hoffstein, J. Pipher and J. Silverman, "NTRU: A ring-based public key cryptosystem," In Algorithmic number theory. Springer, 1998, pp.267–288.

[27] N. Howgrave-Graham," Finding small roots of univariate modular equations revisited," Crytography and Coding (1997), 131–142.

[28] N. Howgrave-Graham, "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU," In Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 150–169.

[29] N. Howgrave-Graham and N. Smart, "Lattice attacks on digital signature schemes," Designs, Codes and Cryptography 23, 3 (2001), 283–290.

[30] G. Hu, Y. Pan and F. Zhang, "Solving random subset sum problem by lp-norm SVP oracle," Public Key Cryptography–PKC 2014 (2014), 399–410.

[31] J. Blömer and A. May, "New partial key exposure attacks on RSA," In Advances in Cryptology-CRYPTO 2003. Springer, 2003, pp. 27–43.

[32] E. Jochemsz and A. May, "A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants," In Advances in Cryptology–ASIACRYPT 2006 (2006), 267–282.

[33] E. Jochemsz and A. May, "A polynomial time attack on RSA with private CRT-exponents smaller than N0.073," In Advances in Cryptology-CRYPTO 2007. Springer, 2007. pp. 395–411.

[34] N. Kunihiro and K. Kurosawa, "Deterministic polynomial time equivalence between factoring and key-recovery attack on Takagi's RSA," Public Key Cryptography–PKC 2007 (2007), 412–425.

[35] N. Kunihiro, N. Shinohara and T. Izu, "A unified framework for small secret exponent attack on RSA," In Selected Areas in Cryptography (2012), Springer, pp. 260–277.

[36] J. Lagarias and A. Odlyzko, "Solving low-density subset sum problems," Journal of the ACM (JACM) 32, 1 (1985), 229–246.

[37] P. Leadbitter, D. Page and N. Smart, "Attacking DSA under a repeated bits assumption," In Cryptographic Hardware and Embedded Systems-CHES 2004. Springer, 2004, pp. 428–440.

[38] G. Leander and A. Rupp, "On the equivalence of RSA and factoring regarding generic ring algorithms," In Advances in Cryptology–ASIACRYPT 2006. Springer, 2006, pp. 241–251.

[39] A. Lenstra, H. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen 261, 4 (1982), 515–534.

[40] M. Liu and P. Nguyen, "Solving BDD by enumeration: An update," In Topics in Cryptology–CT-RSA 2013. Springer, 2013, pp. 293–309.

[41] U. Maurer, "Abstract models of computation in cryptography," In Cryptography and Coding. Springer, 2005, pp. 1–12.

[42] A. May, "Cryptanalysis of unbalanced RSA with small CRT-exponent," In Advances in Cryptology–CRYPTO 2002 (2002), 221–244.

[43] A. May, "New RSA vulnerabilities using lattice reduction methods," PhD thesis, 2003.

[44] A. May. and M. Ritzenhofen, "Solving systems of modular equations in one variable: how many RSA-encrypted messages does eve need to know?," In Public Key Cryptography–PKC 2008 (2008), Springer, pp. 37–46.

[45] A. May. and M. Ritzenhofen, "Implicit factoring: On polynomial time factoring given only an implicit hint," Public Key Cryptography–PKC 2009(2009), 1–14.

[46] G. Miller, "Riemann's hypothesis and tests for primality," In Proceedings of seventh annual ACM symposium on Theory of computing (1975), ACM, pp. 234–239.

[47] P. Nguyen, "Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97," In Advances in Cryptolog-CRYPTO'99 (1999), Springer, pp. 288–304.

[48] P. Nguyen and I. Shparlinski, "The insecurity of the digital signature algorithm with partially known nonces," Journal of Cryptology 15, 3 (2002),151–176.

[49] Y. Pan and Y. Deng, "A ciphertext-only attack against the Cai-Cusick lattice-based public-key cryptosystem," IEEE Transactions on Information Theory 57, 3 (2011), 1780–1785.

[50] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," In Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on (1982), IEEE, pp. 145–152.