Unique Rabin-Williams Signature Scheme Decryption

Lynn M. Batten[1][0000-0003-4525-2423] and Hugh C. Williams[2]

[1] Deakin University, Geelong, Victoria, Australia

[2] University of Calgary, Alberta, Canada

Abstract. The extremely efficient Rabin-Williams signature scheme relies on decryption of a quadratic equation in order to retrieve the original message. Customarily, square roots are found using the Chinese Remainder Theorem. This can be done in polynomial time, but generally produces four options for the correct message which must be analyzed to determine the correct one. This paper resolves the problem of efficient deterministic decryption to the correct message modulo p^2q by establishing conditions on the primes p and q as well as on any legitimate message. We do this using the CRT modulo pq to find four roots. We show that the correct root (initial message) is the only one of these four which is in our allowed message set (it is in fact the smallest of the four integers) and which satisfies a quadratic equation modulo p^2q; no additional work is required to eliminate the others. As a result, we propose what we believe is now the most efficient version of R-W signature scheme decryption.

Keywords: Rabin-Williams, CRT, Signature Scheme.

1. Motivation

In 1979, Rabin promoted a variation of RSA using the encryption exponent 2, and claimed that a signature verification based on his ideas is 'several hundred times faster than for the general RSA scheme'[17]. He also proved that forging Rabin signatures is equivalent to factoring the modulus, which is a product of two prime numbers. In order to verify the signature, decryption is required and is achieved by using the Chinese Remainder Theorem (CRT) [14; section 2.4.3], which in general results in four possible solutions.

Examining Rabin's scheme, Williams [21] noted that the use of special prime types would make the scheme more efficient. In particular, he uses primes p and q congruent to 3 and 7 modulo 8 respectively, and he restricts the message space to a certain set. While decryption still leads to four values, he is able to distinguish from these the 'correct' one by means of quadratic residue theory. More details are given in our Section 2.

Since 1980, the Rabin scheme as adapted by Williams, has become known as the 'Rabin-Williams public-key signature scheme' which is one of the most efficient variations of RSA known to date. In fact, in [5; Introduction], Bernstein states: "Variants of the Rabin-Williams public-key signature system have, since 1980, held the speed records for signature verification." See also his comments in [3] on 'The world's fastest digital signature system' which includes comments about the comparative speeds of signature checking variations using 2-adic divisibility. The Rabin-Williams scheme, sometimes referred to as the 'R-W signing technique' or the 'modular square root (MSR) technique' is still used in recent papers as a fast method of providing authentication, especially useful in low resourced environments.

One of the problems in using the CRT to locate square roots is that with a modulus which is a product of two primes, four square roots are always located. As mentioned in [6] and

[12], the question of how to choose the correct one is an issue. Additional checking to determine the correct one is possible, and in fact was done by Williams in 1980 as mentioned above, but this leads to less efficiency in using the signature scheme.

The authors of [6] give a comprehensive overview of the variations on Rabin's protocol along with their benefits and faults. They explain that their reason for focusing once again on the work in [16] is because of the efficiency of a simple squaring for encryption and because Rabin proved that its security is equivalent to factoring the modulus $n = pq$. They point out that its major drawback is the four-to-one mapping which necessitates additional work to correctly decrypt, particularly when using it as a signature scheme. Their Section 3 reviews the variants of [16] based on a modulus which is a product of two primes both congruent to 3 modulo 4, including R-W. All variants presented in that section rely on the Jacobi symbol or on Dedekind sums, use the CRT to generate four potential roots, and use additional work to determine the correct root. Section 4 of [6] examines possibilities that would extend the Rabin scheme to other types of primes. The case where $x^2 \equiv m \pmod{n}$ has no solution is considered in their Section 5.

In [12], the authors also attempt to solve the problem of uniquely identifying the correct root when using the CRT. They present two ways of doing this, both using the modulus p^2q, for primes p and q with certain conditions; nevertheless, the second method only shows probabilistic uniqueness, as a function on the bounds of p, q and the message used (see Case 1 of Proposition 3.2 of their paper). In addition, in both scenarios, their algorithms 6 and 9 need to check all four options, reducing efficiency once again. None-the-less, the use of modulus p^2q gave the current authors the idea of developing a new variation of R-W which results in a deterministic identification of the correct decryption requiring no computation additional to the polynomial time required to find four potential solutions using the CRT.

In this paper, we resolve the problem of efficient decryption to the correct message modulo p^2q by establishing conditions on the primes p and q, a bound on any legitimate message and then using the CRT modulo pq to find four roots. We show that the correct root (initial message) is the only one of these four which is in our allowed message set and is easily identified because it is the smallest; no additional work is required to eliminate the others. To our knowledge, this is now the most efficient version of R-W signature scheme decryption.

1.1 Our Contribution

1. We propose a version of an R-W signature scheme, which, compared to all other such proposals, has the most efficient decryption method.

2. We show that breaking our scheme is equivalent to factoring $N = p^2q$, for primes p and q.

Section 2 describes the signing protocols of Rabin and of Williams and also a more recent take on these by Bernstein. In Section 3, we mention the security of these schemes. Section 4 reviews other work about signature schemes based on a modulus of the form p^2q.

Section 5 is the main contribution of this paper in which we prove our claims, culminating in Theorem 1 which is followed by an example. Comparison of 5 protocols based on several

features is provided in Section 6, while Section 7 discusses the security of our new scheme proposal. Section 8 is a brief summary.

2. The Schemes of Rabin, Williams and Bernstein

Rabin and Williams use properties of the Jacobi and Legendre symbols, details of which can for instance be found in [14; section 2.4.5]. For completeness, we include the definition relative to an odd prime p here.

For an odd prime p that does not divide an integer a, define the ***Legendre symbol*** (a/p) by

$(a/p)=1$ if there exists an integer x such that $x^2 \equiv a \pmod p$;

$(a/p)=-1$ otherwise.

It can be shown that $(a/p) \equiv a^{(p-1)/2} \pmod p$, whence, $(ab/p)=(a/p)(b/p)$.

RSA tends to be implemented with a large exponent, but Rabin advocated a scheme with $e=2$. He also introduced the use of hashing as a security measure.

2.1 Rabin's protocol

- Bob produces at random two large odd primes p, q and computes $n=pq$ with $2^L<n<2^{L+1}$. (Rabin suggested $L= 1024, 2048, 3072$).
- Bob selects some b, where $0<b<n$. His public key is (n, b).
- To sign a message M, Bob first selects at random a suffix r $(0<r<2^B)$ for a fixed B. (Rabin suggested $B=60$.) He then computes $h=Hash(M||r)$.
- If possible, Bob solves the quadratic congruence
  $$x(x+b) \equiv h \pmod n$$
  for some $s \pmod n$. If this is not possible, change r and try again. (The expected number of trials is 4.) He sends his signature (M,s,r) to Alice.
- Alice verifies Bob's signature by computing $h=Hash(M||r)$ and testing that
  $$s(s+b) \equiv h \pmod n.$$

Notice that Bob could use 3 other possible candidates for s, each of which is tested in Rabin's scheme.

Lemma [16] Breaking Rabin's scheme is essentially equivalent in difficulty to factoring the modulus n.

Proof. Clearly, factoring n will break the scheme.
To see the converse, put $m= h+d^2$, where $d \equiv ((n+1)/2)b \pmod n$; then $x(x+b) \equiv h \pmod n$ if and only if $(x+d)^2 \equiv m \pmod n$.
Suppose we have an algorithm A that finds one of the solutions of $y^2 \equiv m \pmod n$ in $C(n)$ steps whenever $(m/p)=(m/q)=1$. We show that A can factor n in expected $2C(n)+2 \log_2(n)$ steps.

Select k $(1<k<n)$ at random such that $gcd(n,k)=1$ and compute $m \equiv k^2 \pmod{n}$. Apply A to m to find k_1 such that $k_1^2 \equiv m \pmod{n}$. We must have $pq \mid (k-k_1)(k+k_1)$.
There are 4 possibilities:
1. $k \equiv k_1 \pmod{p}$, $k \equiv k_1 \pmod{q}$ with probability $1/4$
2. $k \equiv k_1 \pmod{p}$, $k \equiv -k_1 \pmod{q}$ with probability $1/4$
3. $k \equiv -k_1 \pmod{p}$, $k \equiv -k_1 \pmod{q}$ with probability $1/4$
4. $k \equiv -k_1 \pmod{p}$, $k \equiv -k_1 \pmod{q}$ with probability $1/4$

If (2) or (4) holds, then $gcd(k-k_1, n) = p$ or q with probability ½. On average at most two choices of k need be tried to factor n. Thus, breaking Rabin's scheme is equivalent in difficulty to factoring n.

Problem: How does Bob solve $x(x+b) \equiv h \pmod{n}$?

This is equivalent to solving $y^2 \equiv m \pmod{n}$, where $m = h+d^2$ and $(m/p)=(m/q)=1$. Thus, if Bob can solve for $y \pmod{p}$ and $y \pmod{q}$, then he can use the CRT to find $y \pmod{m}$ and put $s \equiv y-d \pmod{m}$. If n is a Blum number ($p \equiv q \equiv 3 \pmod{4}$) [14; section 2.4.6], finding $y \pmod{p}$ and $y \pmod{q}$ is easy by putting $y \equiv m^{(p+1)/4} \pmod{p}$ and $y \equiv m^{(q+1)/4} \pmod{q}$. Note that $y^2 \equiv m^{(p+1)/2} = mm^{(p-1)/2} \equiv m(m/p) = m \pmod{p}$.

The CRT in this case can be written as: If $y \equiv a \pmod{p}$ and $y \equiv b \pmod{q}$, then

$$y \equiv a + q(q^{-1}(a-b) \pmod{q}) \pmod{pq},$$

where $q^{-1}q \equiv 1 \pmod{p}$ where $q^{-1} \equiv q^{p-2} \pmod{p}$.

Chosen Message Attack: As in most signature schemes, the use of hashes and random numbers must be used to avoid certain attacks. If Bob were to use Rabin's scheme, but neglect to use hashing and randomization, then he might be vulnerable to attack. For, suppose Eve selects some k and computes $M \equiv k(k+b) \pmod{n}$ and asks Bob to sign M to produce (M, s). Since $M \equiv s(s+b) \pmod{n}$, we have $pq \mid (x-k)(x+k+b)$ which means that Eve can factor n with probability $1/2$). Rabin avoids this attack by randomizing and hashing, leaving Eve with no control over the congruence that Bob will solve.

2.2 Williams' protocol

As mentioned earlier, one of the difficulties with Rabin's protocol is that for a given value of a there are four possible values of x satisfying $0<x<n$ and $x^2 \equiv a \pmod{n}$, when this congruence has a solution. This problem can be circumvented by using an idea in Williams [21]. We give a simple précis of this process here with encryption exponent $e=1$ and Alice and Bob interchanged.

Let $n=pq$, where and p and q are primes such that $p \equiv 3 \pmod{8}$ and $q \equiv 7 \pmod{8}$. Williams' protocol is based on the observation that the Jacobi symbol $(a|n)$ can be easily evaluated without knowing the factorization of n. For more information about evaluating the Jacobi symbol, see Shallit [17].

The protocol is dependent of the following simple result.

Theorem. For a given integer C such that $(C/n)=1$, then $C^{(p-1)(q-1)/4} \equiv \pm 1 \pmod{n}$.

Put $\mathcal{X}=\{x: 4(2x+1)<n \text{ and } (2x+1|n)=1 \text{ OR } 2(2x+1)<n \text{ and } (2x+1|n)=-1\}$. If $x \in \mathcal{X}$, we define $E(x)= 4(2x+1)$ when $((2x+1)/n)=1$, or $E(x)= 2(2x+1)$ otherwise. Observe that since $n \equiv 5 \pmod 8$, we always have $(E(x)/n)=1$ for $x \in \mathcal{X}$. In [21] it is shown that $|\mathcal{X}| \approx 3(p-1)(q-1)/16$ which means that if we select at random some x such that $0<2(2x+1)<n$, there is a good chance that $x \in \mathcal{X}$.

Set $d=((p-1)(q-1)/4+1)/2 = m$, so that, with $e=1$, $ed \equiv m \pmod{\text{lcm}(p-1, q-1)}$ as in [21].

The Williams "Signing Protocol"

- Bob produces at random two large primes p, q such that $p \equiv 5$ and $q \equiv 7 \pmod 8$. He next computes $n=pq$ with $2^L<n<2^{L+1}$. The value of n is made public.
- To sign a message M, Bob first selects at random a suffix r ($0<r<2^B$) for a preselected B and then computes $h=Hash(M||r)$. If $h \notin \mathcal{X}$, change r and try again until we find some $h \in \mathcal{X}$. In view of previous remarks, only a few trials should suffice.
- Bob computes $S \equiv h^d \pmod n$ where $0<S<n$. He then sends his signature (M, S, r) to Alice.
- Alice determines $h=Hash(M||r)$ and verifies that $h \in \mathcal{X}$. She then computes L such that $0<L<n$ from $L \equiv S^2 \pmod n$. (This step is not mentioned in [W1980], but is consistent with the method of [R1979].)

She can verify the signature by the following simple procedure:

If $L \equiv 0 \pmod 4$, she checks that $M=(L/4-1)/2$;
if $L \equiv 1 \pmod 4$, she checks that $M=((n-L)/4-1)2$;
if $L \equiv 2 \pmod 4$, she checks that $M=(L/2-1)/2$;
if $L \equiv 3 \pmod 4$, she checks that $M=((n-L)/2-1)/2$.

Alice is able to determine the unique L because of the following result:

Theorem. For a given integer C, there is only one solution L $(0<L<n)$ of the congruence

$$X^2 \equiv C \pmod n \qquad (*)$$

such that $2 \nmid L$ and $(L|n)=1$.

Proof. Let N_1, N_2, N_3, N_4 be the four distinct solutions of (*) such that $0< N_1, N_2, N_3, N_4<n$. since $n-N_i$ is a solution of (*) whenever N_i is, we see that only 2 of N_1, N_2, N_3, N_4 are even; without loss of generality, suppose they are N_1 and N_2. We have $N_1^2 \equiv N_2^2 \equiv C \pmod n$ which implies that $n|(N_1^2-N_2^2)$ or $n|(N_1+N_2)(N_1-N_2)$. Since n cannot divide both N_1+N_2 and N_1-N_2, we must have $p|(N_1-N_2)$ and $q|(N_1+N_2)$. Hence, $(N_1|p) = (N_2|p)$ and $(N_1|q) =(-N_2|q)= -(N_2|q)$, and therefore $(N_1|pq) = -(N_2|pq)$. Hence only one of the even solutions satisfies the necessary Jacobi symbol equation.

Much later than Williams' paper of 1980, Kurosawa and Ogata in [10] developed a scheme they claimed improved Rabin's scheme by deterministically identifying the 'correct' message as well as by running much more efficiently. Their setup is very similar to that of Williams, and like Williams, deterministically identifies the message wanted. Their real

contribution appears to be an improvement in the speed with which the signature scheme runs.

2.3 Bernstein's protocol

Williams [21] modified Rabin's scheme by replacing a square root s by, what Bernstein [4] refers to as a 'tweaked square root', a triple which speeds up signing. Bernstein explains the reason: "Recall that Rabin's system needed to try several values of r, on average about 4 values, before finding a square h = Hash(M||r) modulo pq." Bernstein's interpretation of the R–W system eliminates this problem by using tweaked square roots in place of square roots. According to Bernstein, a ***tweaked square root of h modulo pq*** is a vector (e, f, s) such that $e \in \{-1, 1\}$, $f \in \{1, 2\}$ and $efs^2 - h \in pqZ$; the signer's secret primes p and q are chosen from $3 + 8Z$ and $7 + 8Z$ respectively. Each h has exactly four tweaked square roots, so each choice of r works, speeding up signatures.

Like Williams, Bernstein adopts the restriction that $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$, under which conditions we have Jacobi symbols $(-1/p) = (-1/q) = -1$, $(2/p) = -1$, $(2/q) = 1$.

With $h=Hash(M||r)$, Bernstein makes use of the following simple theorem.

Theorem. [4] Given any h, there exists (e, f, x) such that $e \in \{1,-1\}, f \in \{1,2\}$ and

$$efx^2 \equiv h \pmod n. \qquad (**)$$

Proof. If suffices to find e and f such that $(efh/p) = (efh/q) = 1$. Since $e \in \{1,-1\}$, we must have $(e/q)=(e/p)=e$. Also, we have $(f/q)=1$; hence, we get $(eh/q)=1$ and $e=(h/q)$. Since $(f/p) = (eh/p) = e(h/p)$, we select $f=1$ when $(h/p) = e$; otherwise, put $f=2$. QED

Bernstein calls a solution of (**) a "tweaked square root of h." There exist exactly 4 distinct positive solutions of (**) which are bounded above by $n = pq$. Only one of these, s, is such that $(s/p)=(s/q)=1$. He calls this the **principal tweaked square root** of h.

Bernstein's protocol is:

- Bob solves (**) for the principal tweaked square root s of h.
- He sends his signed message (M, e, f, r, s) to Alice.
- Alice computes $h=Hash(M||r)$
- She then computes $efs^2 \pmod n$ and checks that this is $h \pmod n$. If so, she accepts that Bob sent M.

Bernstein's algorithm from [4] to solve (**) for the principal tweaked square root s of h (mod $n = pq$) is copied in here:

Since $(s/p)=(s/q)=1$, there must exist some y such that $s \equiv y^2 \pmod n$. We need to solve $efy^4 \equiv h \pmod n$ for $y \pmod n$.

1. Precompute $2^{(9p-11)/8} \pmod p$, $2^{(3q-5)/8} \pmod q$, $q^{p-2} \equiv q^{-1} \pmod p$.
2. Put $u \equiv h^{(q+1)/8} \pmod q \Rightarrow u^4 \equiv (h/q)h \pmod q \Rightarrow u^4 \equiv eh \pmod q$.
3. If $u^4 \equiv h \pmod q$, put $e=1$; otherwise, put $e=-1$.

4. Put $v \equiv (eh)^{(p-1)/8} \pmod p \Rightarrow v^4 \equiv (eh)^{-1}(eh/p) \Rightarrow (eh)^2 v^4 \equiv (eh)(eh/p) = eh(f/p)$.
5. If $v^4 \equiv eh$, put $f=1$; otherwise, put $f=2$.
6. Put $w \equiv f^{(3q-5)/8} u \pmod q$, $z \equiv f^{(9p-11)/8} v^3 eh \pmod p \Rightarrow efw^4 \equiv h \pmod q$, $efv^4 \equiv h \pmod p$.
7. Now $(3q-5)/2 = q-2+(q-1)/2$ and $(9p-11)/2 = 4p-5+(p-1)/2$
8. Then set $y \equiv (w + q(q^{-1}(z-w) \pmod p)) \pmod n$ and $s \equiv y^2 \pmod n$.

The most expensive steps are (2) and (4), but these are modular exponentiations where the moduli are of only ½ $\log_2 n$ bits. This algorithm does not require Jacobi symbol computations and is high speed.

Bernstein goes on to mention that a square root s of h modulo pq should be transmitted as (s, t) where s and t satisfy $s^2 - tpq = h$, doubling the space taken by signatures but allowing extremely fast verification.

Stinson [18; Section 7.1] and Bernstein [4] explain the need for use of hash functions with signatures in order to avoid some kinds of attacks on them. RSA in its original version did not use hash functions, while Rabin [16], Williams [21] and Bernstein [4] do. In practice these days, all signature schemes sign hashes.

3. Security of these Three Schemes

Both RSA and R-W signature schemes rely on the inability to factor the composite modulus. RSA does this by increasing the size of values used beyond the capability of current factoring algorithms. It has long been well known that factoring the modulus easily breaks RSA [14; section 8.2.2]; however, only recently, in 2016, Aggarwal and Maurer proved that breaking RSA generically is equivalent to factoring [2].

DEFINITION. A security reduction proof for a signature scheme is said to be ***tight*** when breaking the signature scheme leads to solving some well established, unsolved problem with probability close to one. A security reduction proof for a signature scheme is said to be ***loose*** when breaking the signature scheme leads to solving some well established, unsolved problem with probability more than zero but not close to one.

Bernstein [5] examines tight and loose security for variations of RSA and of R-W signature schemes. His analysis shows that if a large number of bits is added to the message before hashing, them both RSA and R-W schemes can be shown to have tight security; in most cases, when at most one bit is added, loose security is the best that can be shown. Surprisingly, variations of the R-W signature scheme are more amenable to tight security proofs than are variations of RSA. In particular, Bernstein demonstrates that the most computationally efficient of all these schemes, the so-called 'fixed unstructured R-W scheme' with no added random bits has tight security.

In [21], Williams proves that the existence of an algorithm for message decryption in his scheme implies one for factoring the modulus which he states as follows:

Theorem [21]. For the message set *M*, encryption function E and modulus n described in Section II of Williams' paper, if there exists an algorithm F such that for every element M

of *M*, F can be applied to find M from E(M), then the following algorithm can be used to factor n.

This is followed by a 4-step algorithm which makes use of F, and gives a proof of the claim.

Bernstein [5] is able to extend this idea to an equivalence for the R-W signature scheme in his Theorem 4.1 which establishes the equivalence of algorithms to compute a tweaked square root and for factoring the modulus. The general overview of his tight security proofs is given in Sections 4 and 5 of his paper, while Sections 6 and 7 go on to treat separately the situations of the number of bits B of r being 0 (in an unstructured scheme) and being > 0 respectively. Hence, his Section 6 proves tight security for unstructured schemes with B = 0; his Section 7 adapts the proof for $B \geq 1$ and for all types of tweaked square roots.

Bernstein does mention that he believes his tight proofs are specific to Rabin-Williams and do not assist with potential tight proofs for RSA.

In Section 7 of our paper, we discuss the security of our new proposal, which is described in detail in Section 5.

4. Public Key Schemes with Modulus p^2q

Some alternative variations on RSA have been given in the literature using $n = p^2q$ as the modulus and attempting to decrypt in this modulus. We describe some of these papers here.

In 1990, Okomoto developed a signature scheme based on two primes, say p and q with modulus $n = p^2q$ [15]. In the paper, Okomoto shows that the scheme's security relies on factoring n. While he mentions [16], he does not use exponent 2, and his focus is on demonstrating that his signature scheme is much faster than those based on RSA.

In 1997 and 1998, Takagi published variations of the RSA scheme also changing the modulus to p^2q, for primes p and q. See [19] and [20]. The aim was to speed up the decryption procedure while retaining security. In establishing the encryption (e) and decryption (d) exponents, Takagi used the equation $ed \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$ which is the same as that used by Williams in [21], though [21] is not mentioned in either of Takagi's papers above.

In [20], Takagi looked at a specific case of the focus of [19] for public key schemes and mentions that his scheme can be used to provide a digital signature, which he claims is faster than an RSA-based digital signature based on the CRT. He also claims that his concept can be used to produce a 'Rabin-type cryptosystem (which) is as intractable as factoring the modulus p^2q.' He proves neither of these claims in this paper, but does mention that, at the time, the difficulty of factoring products of the form p^2q was considered an open problem.

The R-W signature scheme is examined in [12] where the authors mention the problem of deriving the correct decrypted message from the four usually obtained by using the Chinese Remainder Theorem. They consider two situations, both using p^2q as the modulus, and provide two methods of producing a single (correct) decryption of the equation $C \equiv X^2 \pmod{p^2q}$. Both methods begin with certain conditions on p and q, restrict the message set, and

use the CRT to determine four solutions to an equation for a square modulo pq (rather than p^2q); neither method uses message redundancy or the Jacobi symbol. While their methods produce a single (correct) decryption to the original message, they are not more efficient than other decryptions of R-W, since, in all cases, four possible solutions are found and then three have to be eliminated. (We refer the reader to their paper, and note that in Algorithm 6, lines 8 and 9, and Algorithm 9, lines 8 and 9, N should be p^2q.)

For primes p and q congruent to 3 modulo 4, the CRT can easily be used to solve an equation modulo p^2q; the two equations derived are modulo p^2 and then q. We sketch the procedure below.

Proposition 19.1 [9; p 104]. Let p be a positive prime integer, and let $k \in N$. If $f(r) \equiv 0 \pmod{p^{k+1}}$ then $f(r) \equiv 0 \pmod{p^k}$. (The proof is trivial.)

Corollary**.** The number of solutions to $x^2 \equiv A \pmod{p^k}$ is the same as the number of solutions to $x^2 \equiv A \pmod{p}$, for p a positive prime integer and $k \geq 1$.

In the same section (19) of [9], this proposition is followed by a version of Hensel's (lifting) Lemma which uses roots from $f(x) \equiv 0 \pmod{p^k}$ to obtain roots of $f(x) \equiv 0 \pmod{p^{k+1}}$. For a univariate function *f*, the notation *f'* denotes the derivative of *f* with respect to its unique variable.

Theorem 19.2 (Hensel's Lemma as in [9; p 104]). Let f(x) be a polynomial of positive degree, and suppose that $f(r) \equiv 0 \pmod{p^k}$, so that $c = f(r)/p^k$ is an integer. Based on the derivative f'of f, Hensel continues with conditions under which roots are related. For instance: If $f'(r) \neq 0 \pmod{p}$ then $f(r + tp^k) \equiv 0 \pmod{p^{k+1}}$ if and only if $t \equiv -c[f'(r)]^{-1} \pmod{p}$. (See [9] pages 104 and 105 for full details.)

Only the statement we need below is quoted here from Theorem 19.2 as given by Klain in [9].

Lemma. Let $p \equiv 3 \pmod 4$ and $0 < A < p$ be an integer such that $\gcd(A, p) = 1$. Then there exist precisely two solutions modulo p^2 to the equation

$$X^2 \equiv A \pmod{p^2} \qquad (***)$$

and these are the negative of each other modulo p^2.

Proof. It is well known that $X^2 \equiv A \pmod p$ has the two solutions $\pm A^{(p+1)/4}$ modulo p, each relatively prime to p. By the Corollary to Proposition 19.1, there are precisely two solutions to $X^2 \equiv A \pmod{p^2}$.
The proof of Theorem 19.2 goes on to describe exactly how to obtain these two solutions. Letting $f(x) = x^2 - A$, we have that $f(\pm A^{(p+1)/4}) \equiv 0 \pmod p$ and so $c = f(\pm A^{(p+1)/4})/p$ is an integer for both $\pm A^{(p+1)/4}$. Now $f'(x) = 2x$ and $f'(\pm A^{(p+1)/4}) = (\pm 2A^{(p+1)/4})$ is not congruent to 0 modulo p since $\gcd(A, p) = 1$. It follows from Theorem 19.2 above that we can compute each of the two solutions $\pm A^{(p+1)/4} + tp \pmod{p^2}$ to (***), where $t \equiv -c[\pm 2A^{(p+1)/4}]^{-1} \pmod p$.

Corollary. (a) For $p \equiv 3 \pmod 4$ and $0 < A < p$ an integer such that $\gcd(A, p) = 1$, the two solutions to the equation (***) can be found in polynomial time.
(b) For p and q primes, $p, q \equiv 3 \pmod 4$ and A an integer such that $\gcd(A, pq) = 1$, the four solutions to $X^2 \equiv A \pmod{p^2q}$ can be found in polynomial time.

Proof. For the first statement, apart from calculating additions and multiplications modulo p and p^2, from the proof of the Lemma, the only division (involving the polynomial time Euclidean Algorithm) is in calculating $t \equiv -c[\pm 2A^{(p+1)/4}]^{-1} \pmod p$. For the second statement, in addition to the first calculation, only the polynomial time CRT is needed to find the four solutions.

5. Our Proposal

In all the papers making use of variations of R-W mentioned above, the CRT is used to determine four solutions of a quadratic equation modulo some function of two primes. In all cases, some final work is needed to ascertain the correct (original) message. This is usually done by applying constraints to the primes and to the message set. In most cases this has been enough to guarantee the identification of the original message. In the case of [12], uniqueness of the correct message is probabilistic only, as a function of the bound n applied to the primes and messages. (See Case 1 of their Proposition 3.2.)

Our aim in this section is to construct an R-W type signature scheme modulo p^2q which deterministically identifies the correct original message more efficiently than do previous schemes.

5.1 Assumptions

We begin with two primes, p and q, (for our main result choosing both congruent to 3 modulo 4), and a fixed positive integer s such that $1 < s < \sqrt{q}$. We will require a message set restricted using this value s. We choose the set $\mathbf{M}$ = {integers $0 < M < pq/s$, with $\gcd(M, pq) = 1$}. Given a message M from $\mathbf{M}$, we suppose $D \equiv M^2 \pmod{p^2q}$. When D is sent as a signed message, we want the recipient to recover the correct message M as efficiently as possible without knowing the sender's secret information. Note that in taking square roots modulo pq, both a root m, and pq-m will satisfy the equation. The next Lemma shows that not both of these roots can be in our restricted message set.

LEMMA 1. Let p and q be primes and s a positive integer such that $1 < s < \sqrt{q}$. Let M be an integer from the set $\mathbf{M}$ = {integers $0 < M < pq/s$, with $\gcd(M, pq) = 1$}. If $M \in \mathbf{M}$, then $pq - M \notin \mathbf{M}$.

Proof. By contradiction, if $pq - M < pq/s$, then, $pq - pq/s < M < pq/s$, so that $1 < 2/s$, while s must be at least 2 by the assumption on it. So this is false.

COROLLARY. Under the conditions of Lemma 1, at most two of the solutions of $D \equiv X^2 \pmod{pq}$ can be in $\mathbf{M}$.

The next theorem, which is our main result, shows how, when choosing primes and messages appropriately, we can isolate the correct message with no work additional to the Euclidean algorithm and CRT computations.

THEOREM 1**.** Let p and q be primes congruent to 3 modulo 4 and let s be an integer such that $1 < s < \sqrt{q}$ and such that $sp > 2q$. Let M be an integer from the set $\mathbb{M}$ = {integers $0 < M < pq/s$, with $\gcd(M, pq) = 1$}. Let $D \equiv M^2 \pmod{p^2q}$. Then M is the only root of

$$D \equiv X^2 \pmod{pq} \tag{1}$$

which is also a root of

$$D \equiv X^2 \pmod{p^2q}. \tag{2}$$

Proof. Note first that any solution to equation (2) is also a solution to equation (1), so M is a root of both equations.
Since p and q are congruent to 3 modulo 4, it is well known, that each of $X^2 \equiv D \pmod{q}$ and $X^2 \equiv D \pmod{p}$ has precisely two solutions. Using the Euclidean Algorithm, in the usual manner, write $\gcd(p, q) = 1$ as a combination of p and q.
These four combinations result in all four solutions to equation (1); label them M_1, M_2, M_3 and M_4. Each M_i is a positive value less than pq and they are all distinct modulo pq (in fact they can be paired as a solution and its negative); recall that the initial integer M is one of these solutions; we show that it is the only one less than pq/s which satisfies both (1) and (2).

We work by contradiction. Suppose that two of the M_i are less than pq/s. Say $pq/s > M_i > M_j > 0$. Since $M_i^{\,2} \equiv M_j^{\,2} \pmod{p^2q}$, it is the case that $p^2q \mid (M_i - M_j)(M_i + M_j)$. We now consider three situations. Let $\alpha = 1$ or -1.

Case 1. $p^2q \mid (M_i - M_j)$ OR $(M_i + M_j)$.

The first division implies that M_i and M_j are the same in this modulus, which is a contradiction. The second implies that they are the negative of each other, more specifically that $M_i = p^2q - M_j$. But both are less than pq/s, so this cannot be the case since $p^2q = M_i + M_j < 2pq/s$ only if $sp < 2$.

Case 2. $pq \mid (M_i + \alpha M_j)$ AND $p \mid (M_i - \alpha M_j)$.

In this situation, $p \mid \{(M_i + \alpha M_j) + (M_i - \alpha M_j) = 2M_i\}$ which is impossible.

Case 3. $p^2 \mid (M_i + \alpha M_j)$ AND $p \mid (M_i - \alpha M_j)$.

Set $(M_i + \alpha M_j) = Sp^2$, for some non-negative integer S. Then $0 \le Sp^2 \le |M_i| + |M_j| \le 2pq/s < p^2$ since by assumption, $sp > 2q$. Therefore $S = 0$ and once again $M_i = \alpha M_j$ which cannot be possible for either value of α.

It follows that the original value M is the only one of the four solutions which is less than pq/s and which satisfies both (1) and (2).

COROLLARY**.** Let p and q be primes congruent to 3 modulo 4 and let s be an integer such that $1 < s < \sqrt{q}$ and such that $sp > 2q$. Let $M \in \mathbf{M}$ = {integers $0 < M < pq/s$, with $\gcd(M, pq) = 1$}. Let $D \equiv M^2 \pmod{p^2q}$. Then M is the smallest root of $D \equiv X^2 \pmod{pq}$.

Proof. This follows from the proof of Theorem 1 as all four solutions M_1, M_2, M_3 and M_4 to $D \equiv X^2 \pmod{pq}$ must be less than pq but only one of these, the original M, is less than the bound pq/s, hence is the smallest.

We conclude this section with an example of THEOREM 1 and its COROLLARY.

EXAMPLE. Bob chooses primes p=1187 and q = 2351, congruent to 3 modulo 4, and $4 = s < \sqrt{q}$; he chooses as his bound B on messages the integer part of pq/s which is 697659. He lets $N = p^2q = 3312486119$, keeps p, q and pq secret and publishes the parameters of his signature scheme as (N = 3312486119, B = 697659).

Alice has a message M to send to Bob using his signature scheme. She makes sure that M is less than B and that gcd(M, N) = 1. Alice chooses M = 500000, computes the signed message $D \equiv M^2 \equiv 1563541075 \pmod{N}$ and sends D to Bob along with a claim that it came from her.

Bob retrieves M from D as follows using his private information.
First he determines the roots of $X^2 \equiv D \pmod{pq = 2790637}$, using the CRT. Separating primes, he first finds roots of the quadratic for p and q separately, which are

$\pm D^{(p+1)/4} = \pm 914 \pmod{1187}$; set $R_1 = 914$, and
$\pm D^{(q+1)/4} = \pm 1588 \pmod{2351}$; set $R_2 = 1588$.

Using the CRT based on these four values, and using Maple commands ([13]) Alice computes the four solutions to the modulo pq equation as:

chrem([R_1,R_2],[p,q]); 1405135 $\notin$ **M**
chrem([R_1,-R_2],[p,q]); 2290637 $\notin$ **M**
chrem([-R_1,R_2],[p,q]); 500000 $\in$ **M**
chrem([-R_1,-R_2],[p,q]); 1385502 $\notin$ **M.**

Finally, by the COROLLARY to THEOREM 1, Bob only needs to choose the correct message as the minimum of these, 500000, which is also the only one in **M.** Note that none of the other solutions to (1) satisfies (2), demonstrating THEOREM 1, and that the value 2290637 appearing in the list of four solutions is in fact pq – 500000 modulo pq. By LEMMA 1, it cannot be less than the bound B.

6. Comparison of Five Rabin-Williams Type Signature Schemes

In his 1979 publication [16], Rabin set the stage by transforming RSA into a useful private key scheme with the efficient encryption exponent 2 as opposed to the very high encryption

exponents usually propounded for RSA. Rabin, Williams [21] and Bernstein [4] employ a method whereby user Bob establishes a private key scheme which incorporates a signature scheme allowing him to send signed messages along with the message in the clear, while permitting the receiver to verify that indeed the message was signed by Bob. In all cases, the receiver needs none of Bob's private information in order to confirm.

The authors of [12] changed this perspective. As in the above schemes, Bob establishes his own private key cryptosystem incorporating a signature scheme which allows ***other*** people to send him signed messages. When Bob receives such a message, he retrieves it using his secret primes along with the CRT. The CRT results in four possible messages, and the authors of [12] indicate how to test each of the four in order to determine which one is correct (the original message). As in the former schemes, Bob posts the signature scheme information allowing anyone to use it to send him a message. The fact that Bob's posted information suffices to identify the message along with the hash of a random value is enough to confirm the identity of the sender.

The work of our paper is along the lines of the [12] paper which can be used similarly as a signature scheme. In our situation Alice needs only to send Bob her signed version of a message and the encrypted message, which, along with his public and private information, allows him to identify the message precisely as well as verify the signature. We improve on [12] by using bounds which uniquely identify (decrypt to) the correct message, without further work, beyond that of using the CRT.

The schemes [15], [19] and [20] discussed in Section 4 are not considered here for the reasons mentioned in that section.

Table 1 compares five schemes both from the point of view of the user setup and of the message recipient. We include items: 'Conditions on primes used', 'Special message set', 'Use of random numbers', 'Number of trials' and 'Work to verify'. Since all five schemes here make use of the CRT to solve quadratic congruence equations in the setup and since no verifier needs the secret primes of another user, we do not include these features in our table. (However, verifiers of signed messages sent to themselves using their own scheme require the secret primes.) Also, since it is recommended in general that public key signature schemes be used with a hash function and some random padding, we do not use these features as distinguishers.

In the table, we assume that Bob has established the scheme and Alice uses it, either as a receiver or as a sender. In the first three schemes, Alice is given the plaintext message and the random value used to produce the hash value, and verifies the signature without knowing the primes; in the last two, Bob uses his secret primes to decrypt the message sent to him by Alice and verifies the signature using a hash provided to him by Alice, along with a random value.

Table 1. Comparison of Five Types of Rabin-Williams Schemes.

	Conditions on primes	**Special message set**	**Random number generation**	**No. trials needed by Bob to set up or verify**	**Work to verify**
IN THE	*SCHEMES*	*FOLLOWING*	*ALICE*	*VERIFIES*	*SIGNATURE*
Rabin [17]	p, q ≡ 3 (mod 4)	No. [0, n) is used for n=pq.	Yes. As message padding.	4 trials by Bob in setting up the scheme.	1 hash 1 congruence
Williams [21]	p ≡ 3 (mod 8) q ≡ 7 (mod 8)	Complex set using Jacobi symbols.	Yes. As message padding.	4 trials by Bob in setting up the scheme.	1 hash 2 congruences 2 lookups 1 Jacobi
Bernstein [4]	p ≡ 3 (mod 8) q ≡ 7 (mod 8)	Same set as in Williams.	Yes. As message padding.	None.	1 hash 1 congruence
IN THE	*FOLLOWING*	*BOB DERIVES*	*SECURE MESSAGE*	*AND VERIFIES*	*SIGNATURE*
[12]	p, q ≡ 3 (mod 4)	No. [0, n) is used for n=pq.	Yes. As message padding.	4 trial divisions by Bob.	1 CRT 4 divisibility checks 1 hash
Our protocol	p, q ≡ 3 (mod 4)	[0, n/s) is used for n=pq and s specially chosen.	Yes. As message padding.	None.	1 CRT 1 hash

In Table 1, a 'trial' refers to elimination of possibilities as in the need to test for values satisfying an equation for Bob in Rabin's protocol and the need to try random numbers to obtain a value in the message set as in Williams' protocol; in both cases, four trials are expected by Bob in order to locate a message in his special message set. In contrast, Bernstein shows how to avoid the need for such trials. In all three of these schemes, the message is sent in the clear and Alice only checks the fact that it has been signed by Bob.

The last two schemes in Table 1 deal with a situation in which Alice can send a confidential signed message to Bob. Only Bob can determine this message and can verify Alice's signature on it. In obtaining the plaintext message using the MAA scheme, Bob applies the CRT, then needs to test all four resulting possibilities for an integer division. In our new protocol, only Bob can determine this message and can verify Alice's signature on it. In obtaining the plaintext message using our scheme, Bob simply applies the CRT with no additional testing.

It is difficult to truly compare all five of these schemes as each is designed either to allow a public key scheme owner to send signed messages to other people, OR to allow others to send the public key scheme owner messages which are to be discovered. None-the-less, two of them use a very complex message set while three use simple message sets.

The final two are able to recover a confidential message directly from a CRT and so are both more functional and more efficient than the first three protocols. However, the MAA protocol needs to do up to four additional checks before determining the message, and in addition, as mentioned in their Proposition 3.2, uniqueness in [12] is only demonstrated up to a probability as a function of the bound chosen on the primes. In contrast, in our new protocol, Bob only needs to apply the CRT to determine the plaintext message and its uniqueness is shown to be with probability 1.

7. Security of our Scheme

In our protocol of Section 5, we can assume that any potential attacker, Eve, understands fully how Bob established his private key and signature schemes. She also has access to the modulus N and bound B. She knows that N has the form p^2q, that B is an integer in the range $(p\sqrt{q}, pq/s)$ where p and q are Bob's secret primes and s is some integer satisfying $1 < s < \sqrt{q}$ and $sp > 2q$. The following theorem establishes the fact that for Eve to break Bob's scheme, she must factor N.

THEOREM 2. Breaking our new scheme is equivalent to factoring $N = p^2q$.

Proof. Clearly, if an attacker Eve can factor $N = p^2q$, then she has Bob's secret primes, thus breaking his scheme.
As mentioned above, an attacker Eve is assumed to have Bob's values N and B and to know precisely how Bob's scheme has been established. Eve's aim is to determine the primes p and q where $N = p^2q$, and $sp > 2q$. Since Bob can allow s to vary while still fixing B as an integer in the range $(p\sqrt{q}, pq/s)$, Eve should avoid trying to determine s. Therefore her best attack is to try to factor $N = p^2q$, which only involves Bob's two primes.

Since factoring $n = pq$ is now known to be equivalent to breaking RSA because of [2], the question becomes: is factoring $N = p^2q$ as difficult as factoring $n = pq$?

In 1994, both of these problems were labelled open questions by the Adleman and McCurley in [1]; in fact they propose factoring n as an open question in their Section 5 (Integer Factoring) and factoring N as an open question in their Section 7 (Squarefree part) and then ask if perhaps, finding a polynomial time algorithm for the latter could be translated in polynomial time into one for the former. In 2003, the authors of [7] looked for methods of factoring RSA-type moduli of more than two distinct primes. Their paper examines if selected attacks on RSA can be extended to the multi-prime case, and how they would perform in the new setting. They concluded that, as the number of prime factors in the modulus increases, the attacks become more complex, apply in fewer instances, or become totally ineffective. Zheng and Takagi in [22] also consider the case of more than two distinct primes, in particular with 'small' differences between them; they show that a modulus which is a product of distinct primes with 'extremely small' differences (less than the modulus to a power of one over the square of the number of its primes) can be factored efficiently.

In the meantime there have been several attempts to find polynomial time attacks given a portion of the bits of the primes involved. Zheng credits Hermann and May [8] with showing that if about 70% of the bits of p are known, then n = pq can be factored in time polynomial in O(lnln(n)). We refer the reader to [11] for a description of their method. Zheng himself in [23] uses the ideas of [8] in showing that knowing about 1/3 of the bits of p when the modulus is $N = p^2q$, is sufficient to factor N in polynomial time. He also gives a unified condition on the minimum number of known bits required to factor a modulus of the general form p^aq^b, $a, b \geq 1$.

As of 2019, there appears to be no polynomial time method of factoring N, the best method being the Number Field Sieve which works in sub-exponential time [23]. We can only conclude that factoring $N = p^2q$ is likely to be as difficult as factoring n = pq.

8. Summary

We proposed a version of an R-W signature scheme, and showed that, compared to all other such proposals, it has the most efficient decryption method. See THEOREM 1, its COROLLARY and Table 1. We also proved in THEOREM 2 that breaking our scheme is equivalent to factoring $N = p^2q$, for primes p and q, and argued that it is highly likely that factoring N is equivalent to factoring n = pq, which has been shown in [2] to be generically equivalent to breaking RSA.

References

1. Adleman, L.M. and McCurley, K.S., 1994, May. Open problems in number theoretic complexity, II. In *International Algorithmic Number Theory Symposium* (pp. 291-322). Springer, Berlin, Heidelberg.
2. Aggarwal, D. and Maurer, U., 2016. Breaking RSA generically is equivalent to factoring. *IEEE Transactions on Information Theory*, *62*(11), pp.6251-6259.
3. Bernstein, D. J. (1997) The world's fastest digital signature system, message 1997Mar1104.27.46.12488@koobera.math.uic.edu posted to sci.crypt (1997). URL: http://groups.google.com/group/sci.crypt/msg/840e777ec0fc5679 *last accessed 2019/5/2.*
4. Bernstein, D. J. (2008) RSA signatures and Rabin-Williams signatures: the state of the art, 2008, URL: http://cr.yp.to/papers.html#rwsota , *last accessed 2019/5/2.*
5. Bernstein, D. J. (2008) Proving tight security for Rabin-Williams signatures*, EUROCRYPT, LNCS 4965,* Springer, pp. 70-87.
6. Elia, M., Piva, M. and Schipani, D., 2015. The Rabin cryptosystem revisited. *Applicable Algebra in Engineering, Communication and Computing*, *26*(3), pp.251-275.
7. Hinek, M.J., Low, M.K. and Teske, E., 2002, August. On some attacks on multi-prime RSA. In *International Workshop on Selected Areas in Cryptography* (pp. 385-404). Springer, Berlin, Heidelberg.
8. Herrmann, M., May, A.: Solving linear equations modulo divisors: On factoring given any bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406-424. Springer, Heidelberg.

9. Klain, Daniel. 'Essentials of Number Theory. Copyright D. Klain 2018. Available at *faculty.uml.edu/dklain/Klain-NumberTheory2018.pdf, last accessed 2019/5/2.*

10. Kurosawa, K. and Ogata, W., 1999. Efficient Rabin-type digital signature scheme. *Designs, Codes and Cryptography*, *16*(1), pp.53-64.

11. Lu, Y., Zhang, R. and Lin, D., 2013, July. Factoring multi-power RSA modulus N= p^r*q with partial known bits. In *Australasian Conference on Information Security and Privacy* (pp. 57-71). Springer, Berlin, Heidelberg.

12. [Corrected version] Mahad, Z., Asbullah, M.A. and Ariffin, M.R.K., 2017. Efficient Methods to Overcome Rabin Cryptosystem Decryption Failure. *Malaysian Journal of Mathematical Sciences*, *11*, pp.9-20. (In Algorithms 4 and 7, N should be p^2q.)

13. Maplesoft 2015, 'User Manual', http://www.maplesoft.com/docu-mentation_center/

14. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied Cryptography*, CRC Press, 1997.

15. Okamoto, T., 1990. A fast signature scheme based on congruential polynomial operations. *IEEE Transactions on Information Theory*, *36*(1), pp.47-53

16. Rabin, M.O., 1979. Digitized signatures and public-key functions as intractable a factorization, *Technical Report LCS/TR-212*, MIT Laboratory for Computer Science, 1979, URL: http://www.dtic.mil/dtic/tr/fulltext/u2/a078415.pdf , *last accessed 2019/5/2.*

17. Shallit, O. J, 1990. On the worst case of three algorithms for computing the Jacobi symbol, *Journal of Symbolic Computation,* **21**, pp. 593-610.

18. Stinson, D. R., Cryptography – Theory and Practice. CRC Press, Boca Raton, USA. 1995. 434pages.

19. Takagi, T., 1997, August. Fast RSA-type cryptosystems using n-adic expansion. In *Annual International Cryptology Conference* (pp. 372-384). Springer, Berlin, Heidelberg.

20. Takagi, T., 1998, August. Fast RSA-type cryptosystem modulo p^kq. In *Annual International Cryptology Conference* (pp. 318-326). Springer, Berlin, Heidelberg.

21. Williams, H.C., A modification of the RSA public-key encryption procedure, *IEEE Trans. Inf. Theory, IT-26*, 1980, pp. 726-729.

22. Yi, X., Siew, C.K., Tan, C.H. and Ye, Y., 2003. A secure conference scheme for mobile communications. *IEEE Transactions on Wireless Communications*, *2*(6), pp.1168-1177.

23. Zheng, M., 2018. Improved Results on Factoring General RSA Moduli with Known Bits. *IACR Cryptology ePrint Archive*, *2018*, p.609.