On the Security of Server Aided RSA Protocols

J. Merkle and R. Werchner
Fachbereich Mathematik
Universität Frankfurt
60054 Frankfurt
Germany
e-mail: merkle@cs.uni-frankfurt.de

October 13, 1997

Abstract

In this paper we investigate the security of the server aided RSA protocols RSA-S1 and RSA-S1M proposed by Matsumoto, Kato and Imai resp. Matsumoto, Imai, Laih and Yen. There a smart card wishes to calculate an RSA signature and wants computational assistance from a untrusted powerful server. We focus on *generic attacks*, that is, attacks that do not exploit any special properties of the encoding of the group elements. The notion of generic attacks has been introduced by Shoup. We prove lower bounds for the complexity of generic attacks on these two protocols and show that the bounds are sharp by describing attacks that almost match our lower bounds. To the best of our knowledge these are the first security proofs for efficient server aided RSA protocols.

1 Introduction

In this paper, we investigate the security of server-aided secret computations of RSA signatures. Consider the following scenario: Let $n = pq$ be an RSA modulus and d, e be a pair of private/public exponents. A smart card stores n and d and needs to sign a message x by computing $y = x^d \bmod n$. This takes $O(\log n)$ multiplications modulo n, which is a heavy task for the card. The solution proposed by Matsumoto, Kato and Imai in [8] is server-aided secret computation (SASC). In their protocol RSA-S1 the main part of the computation is done by a more powerful server.

The RSA-S1 Protocol

0. (Preprocessing step) The card chooses an integer vector $\mathbf{d} = (d_1, \ldots, d_m) \in \mathbf{Z}^m$ and a vector $\mathbf{f} = (f_1, \ldots, f_m) \in \{0, 1\}^m$ with Hamming weight k so that $d = \sum_{i=1}^{m} f_i d_i \bmod \phi(n)$.
1. The card sends x, n and $\mathbf{d}$ to the server.
2. The server returns $z_i = x^{d_i} \bmod n$ for $i = 1, \ldots, m$.
3. The card computes the signature y as $y = \prod_{i=1}^{m} z_i^{f_i} \bmod n$.

Consequently Matsumoto, Imai, Laih and Yen proposed a two-phase version of this protocol, called RSA-S1M ([7]).

There exist two kinds of attacks against such protocols: classical searching ones are called *passive attacks*; specific ones where the server returns false values to get some information from the card are called *active attacks*. In [6] Lim and Lee showed, that active attacks can be avoided efficiently. In this paper we focus on the computational complexity of *generic attacks* against RSA-S1 and RSA-S1M — that is, passive attacks, which do not exploit any special properties of the encoding of the elements of $\mathbf{Z}_n$. A similar class of algorithms has been analysed by Shoup ([15]). He proved lower bounds for the complexity of generic algorithms for the discrete log and related problems.

We prove an average case lower bound of $\Omega(N^{1/2})$ for generic attacks against RSA-S1. Here N is the number of possible cointosses of the card. In addition we prove a lower bound of $\Omega(N^{3/4})$ for meet-in-the-middle attacks against RSA-S1M, which have been the most successful attacks so far. Both bounds are asymptotically sharp.

Kawamura and Shimbo ([5]) and Quisquater and de Soete ([11]) proposed rather different SASC protocols. There the communication between the server and the card is independent of the secret key and consequently they are as secure against passive attacks as RSA. Unfortunately these protocols are not efficient. Our results are the first security proofs for efficient SASC protocols.

The structure of the paper is as follows: In section 2 we define SASC protocols and the model of computation. In sections 3 and 4 we review the considered protocols and investigate their security. Finally in section 5 we discuss our results giving some concrete examples and shortly discuss active attacks.

2 Model of Computation

2.1 Server Aided Secret Computation

Let n be a product of two large primes, $d \in \mathbf{Z}^*_{\phi(n)}$ and $x \in \mathbf{Z}^*_n$. Furthermore let the security parameters of the protocol be fixed. In order to compute $x^d \bmod n$ using the help of a server the client carries out the following protocol with the server. In a preprocessing step the client generates some secret (I_s) and some public infomation (I_p) using a fixed randomized algorithm. When the client wants to sign a message he contacts a server. For a fixed number of times he sends him some information and receives an answer. This information depends on the security parameters, the public information generated in the preprocessing and the previous responses of the server. At the end the client computes the signature y using the information responded by the server and his private information generated in the preprocessing. If both parties follow the protocol the result is correct, i.e. $y = x^d \bmod n$.

2.2 Generic Attacks

In [9] Nechaev investigated the complexity of the discrete log problem. Given a finite abelian group G and a fixed generator g of G this is the problem to compute for any $a \in G$ an integer x with $g^x = a$. Nechaev considered algorithms that only perform two kinds of operations on elements of G, multiplication and equality testing.

In [15] Shoup proved lower bounds for the complexity of the discrete log in $\mathbf{Z}_n$ and the Diffie Hellmann problem. He considers algorithms that do not have any computational restriction but get their input (g, g^x) encoded by a randomly chosen function σ. Furthermore they have access to an oracle, which on input $\sigma(g^a), \sigma(g^b)$ outputs $\sigma(g^{a+b})$ or on input $\sigma(g^a)$ outputs $\sigma(g^{-a})$. Shoup calls this kind of algorithms generic. The class of these algorithms can be seen as those that do not depend on the representation of the group G.

These models are closely related and both authors prove a lower bound $\Omega(\sqrt{p})$ for the discrete log problem, where p is the greatest prime divisor of $ord(G)$. We adapt the model of generic algorithms to prove lower bounds for the server aided RSA protocols.

Let n, x, y, d be as above and r, s be distinct primes dividing $\phi(n)$. Further let S be a set of bit strings of cardinality at least n and σ be an injective map from $\mathbf{Z}_n$ to S, the encoding function. A *generic attack* against the server aided RSA protocol is an algorithm which for randomly chosen x, d, σ takes as input $\sigma(x)$ and $\sigma(y)$. It is required to output a value d' with $x^{d'} = x^d \bmod n$. During the computation the algorithm consults an oracle, which on input (a, b) returns $\sigma(y^a x^b)$. (This oracle is more powerful than that in the Shoup model.)

For fixed x and I_p let δ be the number of oracle queries of the algorithm and ρ its probability of success over randomly chosen I_s and a randomly chosen encoding function σ. Then the complexity of the algorithm is defined by the expectation of δ/ρ, over randomly chosen x and I_p.

In practice an adversary can't take advantage of equations $x^\alpha = y^\beta \bmod n$, unless β divides α. The most obvious way to avoid this problem, is to look for equations with $\beta = 1$, like in the meet-in-the-middle attacks of Pfitzmann and Waidner ([10]) or Lim and Lee ([6]). We formalize this type of attack.

We call a generic attack a *meet-in-the-middle attack* iff in all oracle queries the value a is binary, i.e. all queries have the form $(0, b)$ or $(1, b)$. These kind of attacks actually cover the so called meet-in-the-middle attacks of Pfitzmann and Waidner ([10]) and Lim and Lee ([6]), which have been the most successful attacks against RSA-S1 resp. RSA-S1M so far.

All known passive attacks against RSA-S1 and RSA-S1M are generic attacks. Generic algorithms may depend on n but not on the public key e. Otherwise the algorithm could give d rightaway without computation. It seems impossible for a real attacker to use I_p and e both, because in the considered protocols they are related by a quadratic equation modulo $\phi(n)$. Since we focus on attacks that exploit the additional information given by the SASC protocols, we consequently disregard the public key.

3 The 1 Round Protocol

Consider the RSA-S1 protocoll, described in section 1. There a weak device (called the client) generates a signature $y = x^d \bmod n$ of a message $x \in \mathbf{Z}_n^*$, using the help of a powerful device (called the server). For the sake of clarity we claim that the Hamming weight of the secret vectors is fixed, but our results hold for more general variants as well (see the remark at the end of this section). We suppose that $\phi(n)$ has two large prime factors r, s so that r^2, s^2 don't divide $\phi(n)$ (e.g. $\phi(n) = 4rs$). This condition always holds for a secure RSA modulus (see [16, page 151]).

In the RSA-S1 protocol the secret information I_s is the vector $\mathbf{f}$ and the public information I_p is the message x and the vector $\mathbf{d}$.

In the preprocessing step $(f_1, \ldots, f_m)$ is chosen uniformly from the set of all 0-1-

vectors with Hamming weight k. We denote this set by X_k. Given the f_i and d, the d_i are generated by a random process as follows. Let j be the largest index i with $f_i = 1$. Then, all d_i with $i \neq j$ are drawn independently according to the uniform distribution on $\{0, \ldots, c \cdot \phi(n)\}$ for a constant integer $c > 1$ and d_j is computed as $d_j = d - \sum_{i=1}^{j-1} d_i f_i \bmod \phi(n)$. The integer c should be chosen not too small to prevent the knapsack attacks discussed in section 5.

For the generation of the f_i and d_i different scenarios are possible. They can either be generated once for each card and stored in the ROM of the card. Or the generation is done by the card while communicating with the server. In the latter case the cards needs to store all f_i but only a constant number of $\log n$ bit numbers. The pros and cons of both methods are discussed in [6].

3.1 The best known Attack on RSA-S1

A trivial attack is to enumerate all $\binom{m}{k}$ canditates $\mathbf{f} \in X_k$, compute $c = \sum_{i=1}^{m} f_i\, d_i$ and check if $x^c = y \bmod n$.

A more sophisticated approach, called the meet-in-the-middle attack, was proposed by Pfitzmann and Waidner [10]. We present a variation of their attack which was proposed by Oorschot and Wiener in [17] and is slightly more efficient.

From the definition of the protocol we have $x^d = \prod_{f_i=1} z_i \bmod n$. Let m, k be even. With probability $\rho := \binom{m/2}{k/2}^2 / \binom{m}{k}$ it holds that $(f_1, \ldots, f_{\frac{m}{2}})$ has Hamming weight $k/2$. For all possible $(f_1, \ldots, f_{\frac{m}{2}})$ with Hamming weight $k/2$ the attack computes

$$\prod_{\substack{f_i=1\\ i \leq m/2}} z_i \bmod n$$

and sorts them. Subsequently for all $(f_{\frac{m}{2}+1}, \ldots, f_m)$ with Hamming weight $k/2$ it computes

$$y \Big(\prod_{\substack{f_i=1\\ i > m/2}} z_i \Big)^{-1} \bmod n$$

and sorts them as well. It is easy to see that if $(f_1, \ldots, f_{\frac{m}{2}})$ has Hamming weight $k/2$ then there is a collusion which reveals d.

Since the complexity of generic algorithms does not count the effort for sorting and checking the equalities the complexity of this attack is $2\binom{m/2}{k/2}/\rho = 2\binom{m}{k}/\binom{m/2}{k/2}$.

3.2 The Security of RSA-S1

The following theorem shows that the complexity of this attack is nearly optimal. Let $\gamma(n) := \phi(\phi(n))/\phi(n)$ and $N := \binom{m}{k}$.

Theorem. 3.1 *Let be n, r, k, m as above so that $(N^2+1)/r < \gamma(n)/\sqrt{2}$. Then any generic attack against RSA-S1 has at least complexity $\gamma(n)N^{1/2}$*

Proof. For a random variable X let $E(X)$ be the expectation of X. Consider the set $Z := \{\mathbf{f} \in X_k \mid \gcd(\sum_{i=1}^m f_i\, d_i, \phi(n)) = 1\}$. It is easy to see that $E(|Z|) = \gamma(n)N$ where the expectation is taken over a randomly chosen $\mathbf{d}$.

For randomly chosen $\mathbf{d}$ the probability that there are two vectors $\mathbf{f}$ and $\mathbf{f}'$ with $\sum_{i=1}^m f_i d_i = \sum_{i=1}^m f_i' d_i \bmod r$ (collision) is at most N^2/r. Furthermore for randomly chosen x the probability that r doesn't divides the order of x is $1/r$. Depending on x and $\mathbf{d}$ let Ψ be $|Z|$ iff there is no collision and r divides the order of x and 0 else. Since $|Z| < N$ we can estimate $E(\Psi) \geq E(|Z|) - N(N^2+1)/r > \gamma(n)N/\sqrt{2}$.

Let n, x and $\mathbf{d}$ be fixed and $\mathcal{A}$ be a generic attack that makes δ oracle queries and has probability (over a randomly chosen $\mathbf{f} \in \mathbf{Z}$) of success ρ. We show that

$$\delta/\rho > \sqrt{2/N}\Psi \qquad (1)$$

For $\Psi = 0$ this is trivial.

Now let $\Psi = |Z| > 0$. Then there is no collision and r divides the order of x. The probability that $\mathcal{A}$ outputs a d' with $d = d' \bmod r$ is at least ρ. For each pair of oracle queries (a_i, b_i), (a_j, b_j) with $a_i \neq a_j \bmod r$ the oracle returns the same value only if $b_i - b_j = (a_j - a_i)d \bmod r$. Since there is no collision this holds with probability (over a randomly chosen $\mathbf{f} \in Z$) at most $1/|Z|$. Therefore the probability that the oracle returns the same value for any pair (a_i, b_i), (a_j, b_j) with $a_i \neq a_j \bmod r$ is at most $\binom{\delta}{2}/|Z|$. On the other hand, since the encoding function is random, the probability that for all pairs (a_i, b_i), (a_j, b_j) with $a_i \neq a_j \bmod r$ the oracle answers are distinct and $\mathcal{A}$ outputs a d' with $d = d' \bmod r$ is at most $1/|Z|$. Thus we get $\delta^2 > 2\rho|Z|$ which implies (1).

Taking expectations on both sides yields the claim.

■

Remark. Theorem 3.1 holds for the non-binary RSA-S1 as well, where the f_i are ℓ-bit integers. In this case the client performs $k + \ell - 1$ multiplications, a generalisation of the described meet-in-the-middle attack has complexity $2\binom{m\ell}{k}\binom{m\ell/2}{k/2}^{-1}$ and we get a lower bound of $\gamma(n)\binom{m\ell}{k}^{1/2}$. In addition Theorem 3.1 holds if $\mathbf{f}$ are chosen from the set of vectors with Hamming weight *at most* k. There the number of possible choices of $\mathbf{f}$ is $N = \sum_{i=1}^k \binom{m\ell}{i}$. Furthermore Theorem 3.1 remains valid if the values a_i of the oracle queries may depend on the public information $\mathbf{d}$.

4 The 2-Round Protocol

To prevent the meet-in-the-middle attack Matsumoto, Imai, Laih and Yen [7] proposed a 2-round server-aided RSA computation protocol called RSA-S1M. We consider a variant where the Hamming weight of the secret vectors is fixed. This restriction is essentiell for our results.

4.1 The RSA-S1M Protocol

Again let n be a product of two large primes and r, s be large prime factors of $\phi(n)$ so that r^2, s^2 do not divide $\phi(n)$. The client wants to sign a message x with his secret key d.

0. (Preprocessing) The client chooses an integer vector $\mathbf{d} \in \mathbf{Z}^m$ and two vectors $\mathbf{f}, \mathbf{g} \in \{0,1\}^m$ with Hamming weight k so that $d = f \cdot g \bmod \phi(n)$ where f, g are defined as $f = \sum_{i=1}^m f_i d_i$ and $g = \sum_{i=1}^m g_i \bar{d}_j$ with $\bar{d}_j = d_j(j + 3m)$. Furthermore the client randomly picks an $h \in \mathbf{Z}_n$ and computes $t = h^{-g} \bmod n$. (To avoid multi-round attacks the client must pick a new h for each execution of the protocol)

1. The client sends x, n and $\mathbf{d}$ to the server.

2. The server returns $z_i = x^{d_i} \bmod n$ for $i = 1, \ldots, m$.

3. The client computes and sends to the server $z = h \cdot \prod_{f_i=1} z_i = h \cdot x^f \bmod n$.

4. The server returns $v_j = z^{\bar{d}_j} \bmod n$ for $j = 1, \ldots, m$.

5. The client computes the signature y as $y = t \cdot \prod_{g_j=1} v_j = t \cdot z^g \bmod n$.

In this protocol the secret information I_s are the vectors $\mathbf{f}, \mathbf{g}$ and the public information I_p is the message x and the vector $\mathbf{d}$.

Again let X_k denote the set of 0-1 vectors with Hamming weight k and set $d(\mathbf{f}, \mathbf{g}) := \sum_{i,j=1}^m f_i\, g_j\, d_i\, \bar{d}_j \bmod \phi(n)$. Since z is a random number it does not reveal any information about d to the server.

The vectors $\mathbf{f}, \mathbf{g}$ are uniformly drawn from X_k. Here we only consider the case where $\mathbf{f} \neq \mathbf{g}$. So there are i' and i'' with $f_{i'} = 1$, $g_{i'} = 0$, $f_{i''} = 0$, and $g_{i''} = 1$. d is uniformly drawn from $\mathbf{Z}^*_{\phi(n)}$. All d_i except $d_{i'}$ are drawn independently and uniformly from $\mathbf{Z}_n$. $d_{i'}$ is chosen so that $\sum f_i\, d_i$ is invertible modulo $\phi(n)$. $d_{i''}$ is chosen so that $\left(\sum f_i\, d_i\right)\left(\sum g_j\, \bar{d}_j\right) = d \bmod n$. Finally x is drawn uniformly from $\mathbf{Z}_n$.

Our protocol differs from the original RSA-S1M ([7]). We insist on a fixed Hamming weight k of $\mathbf{f}$ whereas in [7] $\mathbf{f}$ is chosen with a Hamming weight up to k and in the second round we let the server use the $\bar{d_j} = d_j(j+3m)$ as exponents instead the d_j. This modifications have technical reasons and do not substantly affect the efficiency of the protocol. In order to achieve a security of 2^{64} we have to insist on an RSA modulus of at least 750 Bit.

4.2 The best known attack on RSA-S1M

In [6] Lim and Lee showed that the ideas of [10] are applicable to RSA-S1M as well. They gave a meet-in-the-middle attack with complexity $O\left(N^{3/4}\right)$, where N was the number of possible pairs $(\mathbf{f}, \mathbf{g})$. We give a variation of this attack which is slighly more efficient and uses ideas of [17].

Let m, k be even. From the definition of the protocol we have

$$x^d = \prod_{f_i=1} x^{gd_i} \bmod n.$$

With probability $\rho := \binom{m/2}{k/2}^2 / \binom{m}{k}$ it holds that $(g_1, \ldots, g_{\frac{m}{2}})$ has Hamming weight $k/2$. The attack guesses $\mathbf{f}$, thereby determines f and for all possible tupels $(g_1, \ldots, g_{\frac{m}{2}})$ with Hamming weight $k/2$ it computes the values

$$\prod_{\substack{g_j=1 \\ j \leq m/2}} v_j \bmod n$$

and sorts them. Subsequently for all $(g_{\frac{m}{2}+1}, \ldots, g_m)$ with Hamming weight $k/2$ it computes the values

$$y \Bigg(\prod_{\substack{g_j=1 \\ j > m/2}} v_j \Bigg)^{-1} \bmod n$$

and sorts them as well. It is easy to see that if $(g_1, \ldots, g_{\frac{m}{2}})$ has Hamming weight $k/2$ then there is a collusion which reveals d.

This attack can be written as a generic attack and has complexity
$2\binom{m}{k}\binom{m/2}{k/2}/\rho = 2\binom{m}{k}^2/\binom{m/2}{k/2}$.

4.3 The Complexity of Meet-in-the-middle Attacks

We show that best known attack against RSA-S1M is optimal for a meet-in-the-middle-attack.

Let $n, r, s, x, \mathbf{d}$ be fixed and let $\mathcal{A}$ be a meet-in-the-middle attack that makes the oracle queries $(a_1, b_1), \ldots, (a_\delta, b_\delta)$ (i.e. $a_i \in \{0, 1\}$ for $i = 1, \ldots, \delta$) and has probability of success ρ over randomly chosen $(\mathbf{f}, \mathbf{g}) \in Z$ and random encoding function σ.

Definition We say that two oracle queries (a_i, b_i), (a_j, b_j) are *related via* $(\mathbf{f}, \mathbf{g}) \in Z$ iff $a_i \neq a_j$ and $y^{a_i} x^{b_i} = y^{a_j} x^{b_j} \bmod n$ holds with $y = x^{d(\mathbf{f},\mathbf{g})} \bmod n$. The latter condition means that the oracle answers of the queries are identical if $d = d(\mathbf{f}, \mathbf{g})$ and implies $b_i - b_j = \pm d(\mathbf{f}, \mathbf{g}) \bmod \operatorname{ord}(x)$. We say that (a_i, b_i), (a_j, b_j) are *related* if they are related via a pair $(\mathbf{f}, \mathbf{g}) \in Z$.

We define a graph $G = (V, E)$ as follows: For every oracle query (a_i, b_i) set a vertex $u_i \in V$. For $i \neq j$ set an edge $(u_i, u_j) \in E$ iff (a_i, b_i) and (a_j, b_j) are related. Due to the particular form of the oracle queries, G is bipartide. The following Lemma reveals the connection between the size of E and the probability of success of the attack.

Lemma. 4.1 *With probability at least* $1 - (4N^2 + r + s)/rs$ *(over randomly chosen* $\mathbf{f}, \mathbf{g}$ *and* σ*) it holds that* $\rho|Z| \leq |E| + 1$.

Proof. Assume that rs divides the order of x. This holds with probability at least $1 - 1/r - 1/s$. Then with probability at least ρ the algorithm outputs a d' with $d = d' \bmod rs$. Further assume that there is no *collision* $d(\mathbf{f}, \mathbf{g}) = d(\mathbf{f}', \mathbf{g}') \bmod rs$ with $(\mathbf{f}, \mathbf{g}) \neq (\mathbf{f}', \mathbf{g}') \in Z$. This holds with probability at least $1 - 4N^2/rs$. Then two oracle queries (a_i, b_i), (a_j, b_j) are related via at most one pair $(\mathbf{f}, \mathbf{g}) \in X_k^2$. Therefore the probability (over randomly chosen $(\mathbf{f}, \mathbf{g}) \in Z$) that there are any related oracle queries is at most $|E|/|Z|$. On the other hand, since the encoding function σ is random, the probability (over randomly chosen $\mathbf{f}, \mathbf{g} \in Z$) that there are no related oracle queries and $\mathcal{A}$ outputs a d' with $d = d' \bmod rs$ is at most $1/|Z|$.

■

Exploiting the nonexistence of certain cycles in G we get a bound for its number of edges. The proof is given in the appendix.

Theorem. 4.2 *Let* $N > 2^{92}$. *Then with probability at least* $1 - 8N^6/rs$ *(over a randomly chosen vector* $\mathbf{d}$*) it holds that* $|V| > 2^{-4.75}|E|N^{-1/4}$.

We are now able to prove the lower bound for the complexity of birthday attacks. Let $\tau := (8N^6 + 2N^2 + r + s)/rs$.

Theorem. 4.3 *Let be n, r, s, m, k as above so that $N > 2^{92}$ and $\tau < \frac{1}{20}\gamma(n)^2$. Then every meet-in-the-middle attack against RSA-S1M has at least complexity $\gamma(n)^2 2^{-5} N^{3/4}$.*

Proof. Using standard arguments, we can estimate $E(|Z|) \geq \binom{m}{k}(\binom{m}{k} - 1)\gamma(n)^2$, where the expectation is taken over a randomly chosen vector $\mathbf{d}$. Since $N \geq 2^8$ this is at least $\frac{19}{20}N\gamma(n)^2$. Depending on x and $\mathbf{d}$ let Ψ be $|Z|$ if Lemma 4.1 and Theorem 4.2 hold, and 0 else. Using $|Z| < N$ we can estimate $E(\Psi) \geq E(|Z|) - \tau N$. Since $\tau < \frac{1}{20}\gamma(n)^2$ and $E(|Z|) > \frac{19}{20}N\gamma(n)^2$ we find that $E(\Psi) > 2^{0.2}N\gamma(n)^2$.

On the other hand by Lemma 4.1 and Theorem 4.2 we get $\delta > 2^{-4.75}(\rho\Psi - 1)N^{-1/4}$. For $\rho\Psi \geq 30$ we get

$$\delta/\rho \geq 2^{-4.8}\Psi N^{-1/4} \tag{2}$$

and since $N \geq 2^{92}$ for $\rho\Psi > 30$ equation (2) is trivial. Taking expectations on both sides yields the claim.

■

Remark. Even if the values a_i of the oracle queries may depend on the public information $\mathbf{d}$, Theorem 4.3 still remains valid.

5 Conclusions

5.1 Discussion of our Results

We give some concrete examples of the sharpness of our results for several choices of the parameters that yield a security of 2^{64}. Since the binary RSA-S1 is not very efficient, we consider the non-binary version. There the f_i are l-bit integers and Theorem 3.1 holds as well. In the case of RSA-S1M , for technical reasons, we suppose that $\phi(n)$ has prime factors r, s fulfilling $rs \gg \binom{m}{k}^{12}$. This holds for a secure RSA modulus of at least 750 bit. But we don't believe that RSA-S1M is less secure for 512 bit moduli.

We compare the upper bound c_1 (given by the described attacks) for the security and the lower bounds c_2 and c_3 (given by our results) for the complexity of a generic resp. a birthday attack against RSA-S1 and RSA-S1M. In the case of RSA-S1 we have $c_2 = c_3$. We omit the terms $\gamma(n)$ and $\gamma(n)^2$. They don't seem to play any role in practice because an attacker does not have much knowledge about $\phi(n)$. The client has to perform $k + l - 2$ resp. $2k + 1$ multiplications.

RSA-S1					RSA-S1M				
m	k	l	c_1	c_2	m	k	c_1	c_2	c_3
80	40	2	$2^{65.4}$	$2^{63.0}$	54	20	$2^{70.9}$	$2^{61.3}$	$2^{66.3}$
92	36	2	$2^{66.1}$	$2^{63.7}$	60	16	$2^{69.2}$	$2^{59.8}$	$2^{64.6}$

These examples show that the bounds of Theorem 3.1 and Theorem 4.3 are quite sharp. The factors $\gamma(n)$ resp. $\gamma(n)^2$ don't seem to play any role in practice because an attacker does not have much knowledge about $\phi(n)$.

5.2 Active Attacks

Various active attacks against the protocols RSA–S1 and RSA–S1M have been proposed in the past (for example see [1],[4],[6]). In an active attack the server returns false values and tries to extract information out of the results presented by the client. As noted in [6] the active attacks can be partially prevented by checking $y = x^d$. This can be done efficiently if e is small by computing y^e. A forged y_i with $f_i = 1$ will be detected. However, using small public exponents can be dangerous in certain circumstances (see [3]). Lim and Lee ([6]) proposed a method to check the equality $y = x^d$ using only 6 multiplication, irrespective of the size of e. We suggest to use this kind of result checking.

However, there are still multi-round active attacks possible. Lim and Lee suggested to change the secret vectors $\mathbf{f}, \mathbf{g}$ and $\mathbf{d}$ randomly after a small number of runs. But in the case of RSA-S1 it is crucial not to choose the vector $\mathbf{d}$ from $\mathbf{Z}_{\phi(n)}^m$ but as integer vectors with components from an intervall $[1, \ldots, c\phi(n)]_{\mathbf{Z}}$ with a constant integer c being large enough. Otherwise the following knapsack–type attack is possible.

Let $d = \sum_{i=1}^m f_i^l d_i^l \bmod \phi(n)$ for $l = 1, 2, \ldots$, where all but one d_i^l are chosen uniformly from $[1, c\phi(n)]$ and the remaining d_j^l is chosen from $[1, \phi(n)]$ so that the equation holds true. Now an attacker can hope that

$$\sum_{i=1}^m f_i^l d_i^l = \sum_{i=1}^m f_i^{l'} d_i^{l'} \tag{3}$$

holds in $\mathbf{Z}$ for small l, l'. In this case using a $2m$ dimensional lattice it is possible to obtain the secret vectors by lattice reduction (see [14],[13]) or max–norm enumeration ([12]). Note that with probability at least $1 - 2^{2m}/(c\phi(n))$ the 0–1 solution of the corresponding knapsack problem is unique.

The following Theorem gives upper and lower bounds for c.

Theorem. 5.1 *For fixed l, l' it holds that* $1/(kc+1) \leq \Pr[(3)] \leq 1/c$.

Proof W.l.o.g. we assume that $f_1^l = f_1^{l'} = \ldots = f_k^l = f_k^{l'} = 1$ and that all d_i^l with $i > 1$ are chosen uniformly from $[1, c\phi(n)]$. Then since d_1 is chosen from $[1, \phi(n)]$ equation (3) holds iff both $\sum_{i=2}^k d_i^l$ and $\sum_{i=2}^k d_i^{l'}$ are in the same intervall $I_j := [d + (j-1)\phi(n), d + j\phi(n) - 1]$ for $0 \leq j \leq kc$. Since the d_i^l are chosen indepentently from the $d_i^{l'}$ we get $\Pr[(3)] = \sum_{j=0}^{kc} \Pr\left[\sum_{i=2}^k d_i^l \in I_j\right]^2$. Setting $x_j := \Pr\left[\sum_{i=2}^k d_i^l \in I_j\right]$ we can write this as $||\mathbf{x}||_2^2$.

Now the first inequality follows from $||\mathbf{v}||_2^2 \geq ||\mathbf{v}||_1^2/t$ for all $\mathbf{v} \in \mathbf{R}^t$ and $t \in \mathbf{N}$.

On the other hand for fixed $d_2^l, \ldots, d_{k-1}^l$ the function $F(d_2^l, \ldots, d_k^l)$ takes $c\phi(n)$ distinct values as d_k^l varies over $[1, c\phi(n)]$. Thus we get $x_j \leq |I_j|/(c\phi(n)) \leq 1/c$ and the second inequality follows from $||\mathbf{v}||_2^2 \leq ||\mathbf{v}||_1 ||\mathbf{v}||_\infty$ for all $\mathbf{v} \in \mathbf{R}^t$.

■

We recommend to choose $c > 2^{80}$ to prevent the described attack. For the RSA–S1M protocol this kind of attack doesn't seem applicable.

A Proof of Theorem 4.2

The case $|E^0| \leq 2^{28}$ is trivial. Before we prove the Theorem for $|E^0| > 2^{28}$, we need some definitions and technical lemmata.

Lemma. A.1 *Let* $\mathbf{f}^1, \mathbf{g}^1, \ldots, \mathbf{f}^8, \mathbf{g}^8 \in X_k$ *with*

$$\sum_{l=1}^{8} (-1)^l \, \mathbf{f}^l \otimes \mathbf{g}^l \neq 0.$$

Let $d_1, \ldots, d_m$ *be independently randomly chosen from* $\mathbf{Z}_{\phi(n)}$. *Then it holds with probability at most* $4/rs$ *that*

$$\sum_{l=1}^{8} (-1)^l \, d(\mathbf{f}^l, \mathbf{g}^l) = 0 \bmod rs. \tag{4}$$

Proof. Equality in (4) is equivalent to equality mod r and mod s. We show that equality mod r holds only with probability $2/r$. Analogously one can see that the probability of equality mod$s$ is $2/s$.

Let equation (4) hold mod$r$. Set

$$\bar{c}_{i,j} = \sum_{l=1}^{8} (-1)^l \, f_i^l \, g_j^l.$$

and, for $1 \leq i < j \leq m$,

$$\begin{aligned} c_{i,j} &= \bar{c}_{i,j}\,(j + 3m) + \bar{c}_{j,i}(i + 3m) \bmod r \\ c_{i,i} &= \bar{c}_{i,i}(i + 3m) \bmod r. \end{aligned}$$

If $\sum_{l=1}^{8}(-1)^l \mathbf{f}^l \otimes \mathbf{g}^l \neq 0$ then there is a $\bar{c}_{i,j} \neq 0$. We show that there is a $c_{i',j'} \neq 0 \bmod r$ as well.

This is obvious for $i = j$. If $i \neq j$ we set $i' = \min(i,j)$ and $j' = \max(i,j)$. Then $c_{i',j'} = 0$ is equivalent to $\bar{c}_{i',j'}\,(j' + 3m) + \bar{c}_{j',i'}(i' + 3m) = 0 \bmod r$. Since $r \gg 32m$ this equation holds in $\mathbf{Z}$ as well and we get $\frac{\bar{i}+3m}{j+3m} = \frac{\bar{c}_{i',j'}}{-\bar{c}_{j',i'}}$. Since the right hand side of the last equation is either equal to 1 or no closer to 1 than 3/4 or 4/3, this equation cannot hold. This shows that $c_{i',j'} \neq 0$.

Now we distinguish two cases. First assume that $i' = j'$. In this case (4) is equivalent to

$$c_{i',i'}(i + 3m)\, d_{i'}^2 + \gamma_1\, d_{i'} + \gamma_2 = 0 \bmod r\,, \tag{5}$$

where γ_1 and γ_2 depend on the $c_{i,j}$ and the d_i $(i \neq i')$. Since $\mathbf{Z}_r$ is a field, equality (5) holds for no more than two out of the r possible values of d_i.

In the second case we have $i' \neq j'$ and $c_{i,i} = 0$ for all i. Fixing all d_i except $d_{i'}$ and $d_{j'}$ (4) becomes

$$c_{i',j'}\, d_{i'}\, d_{j'} + \gamma_1\, d_{i'} + \gamma_2\, d_{j'} + \gamma_3 = 0 \bmod r \tag{6}$$

with certain constants $\gamma_1, \gamma_2, \gamma_3$. Interpreting the left hand side as a linear function in $d_{i'}$ the coefficient of $d_{i'}$ is $c_{i',j'}\, d_{j'} + \gamma_1$. This coefficient is nonzero with probability $1 - 1/r$. But in this case the linear function computes zero on a random $d_{i'}$ also with probability $1 - 1/r$. Thus the probability of (6) holding mod$r$ is at most $2/r$.

■

Definition. For an edge (x, y) labeled by $\mathbf{f}, \mathbf{g}$ we call $\mathbf{f}$ the F-colour and $\mathbf{g}$ the G-colour of (x, y) and write $\mathbf{f} = F(x, y)$, $\mathbf{g} = G(x, y)$. For any $\mathbf{f}, \mathbf{g} \in X_k$ there are at most $\binom{m}{k}$ edges of F-colour $\mathbf{f}$ and $\binom{m}{k}$ edges of G-colour $\mathbf{g}$. A path in G is *colourful* iff it neither all its edges are of the same F-colour nor all its edges are of the same G-colour.

Now suppose $\mathbf{d}$ to have no collision $d(\mathbf{f}, \mathbf{g}) = d(\mathbf{f}', \mathbf{g}')$ with $(\mathbf{f}, \mathbf{g}) \neq (\mathbf{f}', \mathbf{g}')$. This holds with probability $1 - \binom{m}{k}^4/rs$. For each edge $(v_i, v_j) \in E$ there exists a pair $(\mathbf{f}, \mathbf{g}) \in X_k^2$ fulfilling $b_i - b_j = (a_j - a_i)d(\mathbf{f}, \mathbf{g}) \bmod rs$. Since there is no collision this pair is unique. We label the edge by this pair. If a pair $(\mathbf{f}, \mathbf{g})$ occurs more than once as a label of an edge in E we remove all but one of this edges.

The main property of G we will exploit is the non-existence of certain 6–cycles (and even certain 8–cyles). We will then prove a variant of the well known general result that graphs with v nodes not containing cycles of length $L \leq 2\kappa$ have

$O(v^{1+1/\kappa})$ edges ([2]) (here we have $\kappa = 3$). The results of non-existence of certain cycles are obtained using the following Lemmata.

Lemma. A.2 *With probability at least* $(1 - 4N^6/rs)$ *(over a randomly chosen* $\mathbf{d}$*) there are no colourful 6-cycles in* G^0*.*

Proof. For every edge disjunct colourful 6 cycle, we get an equation

$$\sum_{l=1}^{3} d(\mathbf{f}^l, \mathbf{g}^l) = \sum_{l=4}^{6} d(\mathbf{f}^l, \mathbf{g}^l) \bmod rs.$$

Thus by Lemma A.1 with probability at least $(1 - 4N^6/rs)$ we get an equation

$$\sum_{l=1}^{3} \mathbf{f}^l \otimes \mathbf{g}^l \ = \ \sum_{l=4}^{6} \mathbf{f}^l \otimes \mathbf{g}^l$$

for every edge disjoint colourful 6 cycle. If the cycle is colourful then f^1, f^2, f^3 are not all equal and g^1, g^2, g^3 are not all equal. We set $A := \mathbf{f}^1 \otimes \mathbf{g}^1 + \mathbf{f}^2 \otimes \mathbf{g}^2 + \mathbf{f}^3 \otimes \mathbf{g}^3$.

If $\mathbf{f}^2 = \mathbf{f}^3$ we can determine $\mathbf{f}^1$ from $(f_1)_j = 1 \iff \sum_{i=1}^m A_{ij} \in \{k, 3k\}$ and $\mathbf{g}^1$ as A^t_j for any j with $\sum_{i=1}^m A_{ij} = k$. This uniqueness of $\mathbf{f}^1 \otimes \mathbf{g}^1$ contradicts the edge disjointness of the cycle. Analogously we can conclude that $\mathbf{f}^1 \neq \mathbf{f}^3$, $\mathbf{f}^1 \neq \mathbf{f}^2$, $\mathbf{g}^2 \neq \mathbf{g}^3$, $\mathbf{g}^1 \neq \mathbf{g}^3$, $\mathbf{g}^1 \neq \mathbf{g}^2$.

Now we assume that the $\mathbf{f}^l$, $(l = 1,2,3)$, are all distinct and the $\mathbf{g}^l$, $(l = 1,2,3)$, are all distinct. First we show that $\mathbf{g}^1, \mathbf{g}^2, \mathbf{g}^3$ are uniquely determined up to permutation by A and therefore $\{\mathbf{g}^1, \mathbf{g}^2, \mathbf{g}^3\} = \{\mathbf{g}^4, \mathbf{g}^5, \mathbf{g}^6\}$.

If there are 3 (as vectors) distinct columns j_1, j_2, j_3 of A with $\sum_{i=1}^m A_{ij_l} = 2k$ for $l = 1,2,3$ then for all $a, b \in \{1,2,3\}$ it holds that $(f_a)_{j_b}$ is 1 iff $a \neq b$ and is 0 iff $a = b$, and $\mathbf{g}^1, \mathbf{g}^2, \mathbf{g}^3$ are uniquely determined up to permutation by
$\mathbf{g}^1 = A^t_{j_3} - A^t_{j_1} + A^t_{j_2}$, $\mathbf{g}^2 = A^t_{j_1} - A^t_{j_2} + A^t_{j_3}$ and $\mathbf{g}^3 = A^t_{j_2} - A^t_{j_3} + A^t_{j_1}$.

If there are no such 3 columns in A then w.l.o.g. $(f_1)_j = (f_2)_j = 1$ implies $(f_3)_j = 1$ for all j.

Now we can conclude that since $\mathbf{f}^1 \neq \mathbf{f}^3$, $\mathbf{f}^2 \neq \mathbf{f}^3$ there are j_1, j_2 with $(f_i)_{j_1} = 1$ iff $i = 1$ and $(f_i)_{j_2} = 1$ iff $i = 2$. Thus there are at least 2 (as vectors) distinct columns j of A satisfying $\sum_{i=1}^m A_{ij} = k$. If there are 3 of them then they are equal to $\mathbf{g}^1, \mathbf{g}^2, \mathbf{g}^2$ and if there are only 2 of them they are equal to $\mathbf{g}^1, \mathbf{g}^2$ and we can easily determine $\mathbf{g}^3$ from A. Again $\mathbf{g}^1, \mathbf{g}^2, \mathbf{g}^3$ are uniquely determined up to permutation by A.

Analogously one can see that $\mathbf{f}^1, \mathbf{f}^2, \mathbf{f}^3$ are uniquely determined up to permutation by A and therefore $\{\mathbf{f}^1, \mathbf{f}^2, \mathbf{f}^3\} = \{\mathbf{f}^4, \mathbf{f}^5, \mathbf{f}^6\}$. We get $\mathbf{f}^1 \otimes \mathbf{g}^1 + \mathbf{f}^2 \otimes \mathbf{g}^2 + \mathbf{f}^3 \otimes \mathbf{g}^3 \ =$

$\mathbf{f}^1 \otimes \mathbf{g}_{i_1} + \mathbf{f}^2 \otimes \mathbf{g}_{i_2} + \mathbf{f}^3 \otimes \mathbf{g}_{i_3}$ with $\{i_1, i_2, i_3\} = \{1, 2, 3\}$. Now considering a j satisfying $(f_1)_j = 0$ and $(f_2)_j = 1$ it is easy to see that $i_k = k$ for $k = 1, 2, 3$.

■

Definition. For $\tilde{V} \subseteq V$ we say that $\tilde{V}$ is *F-monochromic* if for every vertex $x \in \tilde{V}$ all edges incident to x are of the same F-colour. For any colour $\mathbf{f}$ and $x \in V$ we define $\tilde{V}^F(\mathbf{f})$ as the set of vertices in $\tilde{V}$ whose incident edges are of the F-colour $\mathbf{f}$. Analogously we define $\tilde{V}$ to be *G-monochromic* and $\tilde{V}^G(\mathbf{g})$ for any colour $\mathbf{g}$.

Lemma. A.3 *With probability at least $(1 - 4\binom{m}{k}^{12}/rs)$ (over a randomly chosen $\mathbf{d}$) for every subgraph $\tilde{G} = (\tilde{V}_1, \tilde{V}_2, \tilde{E})$ of G with F-monochromic $\tilde{V}_1$ the following fact holds:*

Fact. A.4 *For any $x_1 \in \tilde{V}_1^F(\mathbf{f}^1), x_2 \in \tilde{V}_1^F(\mathbf{f}^2)$ the number of 4-paths (x_1, a, b, c, x_2) with $F(x_1, a) \neq F(a, b)$ and $F(b, c) \neq F(c, x_2)$ is bounded by*

- $2M$ *if* $\mathbf{f}^1 \neq \mathbf{f}^2$,
- $2Md(x_2)$ *if* $\mathbf{f}^1 = \mathbf{f}^2$,

where $M := \max_{\mathbf{f}}(|\tilde{V}_1^F(\mathbf{f})|)$.

Proof. Let there be 2 such 4-paths from x_1 to x_2. Since $\tilde{V}_1$ is F-monochromic for every such 8 cycle we get an equation

$$\sum_{l=1}^{4}(-1)^l d(\mathbf{f}^l, \mathbf{g}^l) = \sum_{l=5}^{8}(-1)^l d(\mathbf{f}^l, \mathbf{g}^l) \bmod rs$$

with $f^1 = f^8, f^4 = f^5, f^2 = f^3, f^6 = f^7$. Thus by Lemma A.1 with probability at least $(1 - 4\binom{m}{k}^{12}/rs)$ we get the equation

$$\sum_{l=1}^{4}(-1)^l \mathbf{f}^l \otimes \mathbf{g}^l = \sum_{l=5}^{8}(-1)^l \mathbf{f}^l \otimes \mathbf{g}^l.$$

We set $A := \sum_{l=1}^{4}(-1)^l \mathbf{f}^l \otimes \mathbf{g}^l$. In A there are at most 3 (as vectors) distinct columns j that contain 1's and -1's:

$$\begin{array}{lll} a) & f_j^1 = f_j^4 = 1 & f_j^2 = 1 \\ b) & f_j^1 = f_j^4 = 1 & f_j^2 = 0 \\ c) & f_j^1 = f_j^4 = 0 & f_j^2 = 1. \end{array}$$

$\mathbf{f}^2$ is determined by an assignment of the cases $a) - c)$ to the columns. For each column j that contains 1's and -1's it is uniquely determined whether it is of type $c)$ or $a) - b)$. Thus there are only 2 possibilities for $\mathbf{f}^2$. Now fix $\mathbf{f}^2$.

1. Let x_1 and x_2 be of different F-colours. We show that $\mathbf{g}^1$ and $\mathbf{g}^4$ are uniquely determined by A and $\mathbf{f}^2$:

If for all j it holds that $f_j^2 = 1 \Leftrightarrow f_j^1 \neq f_j^4$ then there are j_1, j_2, j_3 so that for all $a, b \in \{1, 2, 3\}$ it holds that $f_{j_b}^a$ is 1 iff $a \neq b$ and is 0 iff $a = b$ and $\mathbf{g}^1, \mathbf{g}^4$ are uniquely determined by $2\mathbf{g}^1 = A_{j_3}^t - A_{j_1}^t + A_{j_2}^t$ and $2\mathbf{g}^4 = A_{j_1}^t - A_{j_3}^t + A_{j_2}^t$.

If there is a j satisfying $f_j^2 = 0$ and $f_j^1 \neq f_j^4$ then A_j^t equals $\mathbf{g}^1$ or $\mathbf{g}^4$ and one can easily determine the other value from A.

2. Let x_1 and x_2 be of the same F-colour. $\mathbf{g}^1$ is uniquely determined by $\mathbf{g}^4$ and A.

For fixed $\mathbf{f}^1 \otimes \mathbf{g}^1$ and $\mathbf{f}^2$ there are at most $|\tilde{V}_1^F(\mathbf{f}^2)|$ many possible values $\mathbf{g}^2$ and $\mathbf{g}^3$ is uniquely determined by $\mathbf{f}^2 \otimes \mathbf{g}^2$ and $\mathbf{f}^4 \otimes \mathbf{g}^4$.

■

Lemma. A.5 *Let $G = (V_1, V_2, E)$ be a graph with $|V_1|, |V_2| \leq v$. For any vertex x let $U(x)$ denote the set of vertices $y \in N(x)$ that are F-dominated. Then G contains a subgraph $\tilde{G} = (\tilde{V}_1, \tilde{V}_2, \tilde{E})$ with $|\tilde{E}| > |E| - 4v \log_2 v$ so that for all $x \in \tilde{V}_1$ it holds that*

$$\max_{y \in U(x)} (d(y) - d_{F(x,y)}(y)) \leq 1/2 \sum_{y \in U(x)} d(y) - d_{F(x,y)}(y) \qquad (7)$$

Proof. We consider the function $D(G) := \sum_{x \in V_1} \sum_{y \in U(x)} d(y) - d_{F(x,y)}(y)$. For every $x \in V_1$ for that (7) doesn't hold we remove the edge (x, y_x) with $y_x \in U(x)$ and $d(y_x) - d_{F(x,y_x)}(y_x) = \max_{y \in U(x)}(d(y) - d_{F(x,y)}(y))$. By that procedure we decrease $D(G)$ at least by a factor of 2. Since $D(G) \leq \sum_{x \in V_1} \sum_{y \in N(x)} d(y)$, which is at most $|E|^2$, we can perform this procedure at most $\log_2(|E|)$ many times.

■

Definition. For a vertex x let $N(x)$ denote the set of vertices y adjacent to x. For $y \in N(x)$ let $d_{F(x,y)}(x)$ denote the number of edges incident to x with F-colour $F(x, y)$. Analogously we define $d_{G(x,y)}(x)$.

For $G = (V, E)$ and $U_1, U_2 \subset V$ we set $E(U_1, U_2) := \{(x, y) \in E \mid x \in U_1 \wedge y \in U_2\}$.

Lemma. A.6 *Let $x \in V$ be colourful and for $y \in N(x)$ let $A_x(y)$ be the set of edges $(x, z) \neq (x, y)$ with $F(x, z) = F(x, y)$ or $G(x, z) = G(x, y)$. Then there is at most one $y \in N(x)$ with $|A_x(y)| > 7/8\, d(x)$.*

The proof follows immediately from $|A_x(y) \cap A_x(y')| \leq 3/4\, d(x)$.

Proof of Theorem 4.2 Assume that $\delta = |V| < 2^{-4.75}|E|N^{-1/4}$. Then, by Lemma A.2 and A.3, with probability at least $1 - N^6/rs$ there is no collision, no colourful 6-cycle and fact A.4 holds. Assume that this is the case and that $|E| > 2^{28}$. Set $V_c := \{x \in V \mid \text{x is colourful}\}$, $V_F := \{x \in V \mid \text{x is F-dominated}\}$ and $V_G := \{x \in V \mid \text{x is G-dominated}\}$.

Subsequently we use variables ϵ_i in the estimations which will be fixed at the end of the proof.

If $|\mathbf{E}(\mathbf{V_F}, \mathbf{V_2})| > \epsilon_\mathbf{1}|\mathbf{E}|$ then G contains a subgraph $G^1 = (V_1^1, V_2^1, E^1)$ so that V_1^1 is F-monochromic and $|E^1| > \frac{3}{4}\epsilon_1|E|$. If the number of F-colours $\mathbf{f}$ satisfying $|V_1^{1,F}(\mathbf{f})| > N^{1/4}$ is greater than $\epsilon_2|E^1|N^{-1/2}$ we have $v > \frac{3}{4}\epsilon_1\epsilon_2|E|N^{-1/4}$.

On the other hand if the number of those colours is at most $\epsilon_2|E^1|N^{-1/2}$ using Lemma A.5 we see that G^1 contains a subgraph $G^2 \subseteq (V_1^2, V_2^2, E^2)$ so that (7) holds for $x \in V_1^2$, for all F-colours $\mathbf{f}$ it holds that $|V_1^{2,F}(\mathbf{f})| \leq N^{1/4}$ and $|E^2| > (1-\epsilon_2)|E^1| - 4v\log_2 v = \alpha_1|E|$. Let $U_2 := \{x \in V_2^2 \mid x \text{ is F-dominated}\}$. There are only two possibilities:

1. If $E^2(V_1^2, U_2) > \epsilon_3|E^2|$ then G^2 contains a subgraph $\tilde{G} = (\tilde{V}_1, \tilde{V}_2, \tilde{E})$ so that $\tilde{V}_1$ and $\tilde{V}_2$ are F-monochromic and $|\tilde{E}| > \frac{3}{4}\epsilon_3|E|$. The number of it's vertices $|\tilde{V}_1| + |\tilde{V}_2|$ is at least $2\sum_\mathbf{f}\sqrt{|\tilde{V}_1^F(\mathbf{f})| \cdot |\tilde{V}_2^F(\mathbf{f})|}$ which is no more than $2N^{-1/4}\sum_\mathbf{f}|\tilde{V}_1^F(\mathbf{f})| \cdot |\tilde{V}_2^F(\mathbf{f})|$. Since $|\tilde{E}| \leq \sum_\mathbf{f}|\tilde{V}_1^F(\mathbf{f})| \cdot |\tilde{V}_2^F(\mathbf{f})|$ we get
$|V| > \frac{3}{4}\epsilon_3\alpha_1|E|N^{-1/4}$.

2. If $|E^2(V_1^2, V_2^2 - U_2)| > (1-\epsilon_3)|E^2|$ we set $\hat{G} = (V_1^2, V_2^2 - U_2, E^2(V_1^2, V_2^2 - U_2))$. Since $\hat{V}_1$ is F-monochromic and $|\hat{V}_1^F(\mathbf{f})| \leq N^{1/4}$ holds for all F-colours $\mathbf{f}$, using fact A.4 we see that the number of 4-paths (x_1, a, b, c, x_2) with $x_1, x_2 \in \hat{V}_1$, $F(x_1, a) \neq F(a, b)$ and $F(b, c) \neq F(c, x_2)$ is bounded by
$\sum\limits_{x_2 \in \hat{V}_1}\left(2N^{1/4}|V| + 2d(x_2)N^{1/4}\right)$, which is at most $4|V|^2N^{1/4}$.

On the other hand since $\hat{V}_1$ is F-monochromic the number of those 4-paths is at least

$$\sum_{(w,x)\in\hat{E}} \sum_{\substack{y\in N(x)\\ F(w,x)\neq F(y,x)}} \sum_{z\in N(y)\setminus\{x\}} d(z) - d_{F(y,z)}(z).$$

Since (7) holds for $x \in \hat{V}_1$, we can estimate this by

$$\begin{aligned} & 1/2 \sum_{(w,x)\in\hat{E}} \sum_{\substack{y\in N(x)\\ F(w,x)\neq F(y,x)}} \sum_{z\in N(y)} d(z) - d_{F(y,z)}(z) \\ = \; & 1/2 \sum_{y\in\hat{V}_1} \Big(\sum_{z\in N(y)} d(z) - d_{F(y,z)}(z) \Big)^2. \end{aligned}$$

Using the Cauchy-Schwarz inequality and that all $z \in \hat{V}_2$ are not F-dominated this is at least $2^{-5}|V|^{-1}\Big(\sum_{(y,z)\in\hat{E}} d(z)\Big)^2$, which equals $2^{-5}|V|^{-1}\Big(\sum_{z\in\hat{V}_2} d(z)^2\Big)^2$. Finally we get the bound $2^{-5}|V|^{-3}|\hat{E}|^4$ which yields $|V| > 2^{-7/5}(1-\epsilon_3)^{4/5}\alpha_1^{4/5}|E|N^{-1/4}$.

If $|\mathbf{E}(\mathbf{V_G},\mathbf{V_2})| \geq \epsilon_1|\mathbf{E_0}|$, $\mathbf{E}(\mathbf{V_1},\mathbf{V_F}) \geq \epsilon_1|\mathbf{E_0}|$ or $\mathbf{E}(\mathbf{V_1},\mathbf{V_G})\mathbf{L_i}| \geq \epsilon_1|\mathbf{E_0}|$ we get the same estimations analogously.

If $\mathbf{E}(\mathbf{V_c},\mathbf{V_c})| \geq (\mathbf{1}-\mathbf{4}\epsilon_1)|\mathbf{E_0}|$ set $G^4 := (V_1, V_2, E(V_c, V_c))$ and let E_4^0 denote the set of edges $(x,y) \in E^4$ with $|A_x(y)| \leq 7/8\, d(x)$ and $|A_y(x)| \leq 7/8\, d(y)$. By Lemma A.6 we get $|E_4^0| > |E_4| - 2|V|$.

Since there are no colourful 6-cycles in G^4 the number of coloured 3-paths, i.e. the paths (w,x,y,z) in G^4 with $w \in V_2^4$, $F(w,x) \neq F(x,y) \neq F(y,z)$ and $G(w,x) \neq G(x,y) \neq G(y,z)$, is at most $|V|^2$.

On the other hand it is at least

$$\sum_{(x,y)\in E_0^4} \Big(d(x) - |A_x(y)|\Big)\Big(d(y) - |A_y(x)|\Big)$$

which is greater than $2^{-6}\sum_{(x,y)\in E_0^4} d(x)d(y)$. Using the identity $\sum_{(x,y)} d(x)^{-1} = \sum_{(x,y)} d(y)^{-1} = |V|$ we can estimate this by $2^{-6}\min\left(\sum a_i b_i \mid \sum a_i^{-1} + b_i^{-1} \leq 2|V|\right)$, where the minimum is taken over all $\vec{a}, \vec{b} \in \mathbf{R}^{|E_0^4|} - \{\vec{0}\}$. The minimum occurs, if all a_i and b_i are equal. Setting $|E_0^4| \geq |E^4| - 2|V| = \alpha_2|E|$ we get the bound $2^{-6}\alpha_2^3|E|^3|V|^{-2}$ which yields $|V| > 2^{-3/2}\alpha_2^{3/4}|E|N^{-1/4}$.

Assume that $|V| < 2^{-4.75}|E|N^{-1/4}$ and $|E| > 2^{28}$. Set $\epsilon_1 = 0.2$, $\epsilon_2 = 0.3$, $\epsilon_3 = 0.5$. Since $N \geq 2^{92}$ we get $\alpha_1 \geq 0.11$, $\alpha_2 \geq 0.2$ and finally $|V| > 2^{-4.75}|E|N^{-1/4}$ which is a contradiction. This completes our proof.

$\blacksquare$

References

[1] R. J. Anderson. Attack on server assisted authentication protocols. *Electronics Letters*, 28(15):1473, 1992.

[2] B. Bollobas. *Extremal graph theory*, volume 11 of *L. M. S. Monographs*, page 158. Academic Press. XX, London, 1978.

[3] J. Håstad. On using RSA with low exponent in a public key network. In *Advances in Cryptology - Proceedings of Crypto'85*, volume 218 of *Lecture Notes in Computer Science*, pages 403–408. Springer Verlag, 1985.

[4] S. Kawamura. Information leakage meassurement in a distributed computation protocol. *IEICE Transactions Fundamentals*, E78-A(11):59–66, 1995.

[5] S. Kawamura and A. Shimbo. Fast server-aided secret computation protocols for modular exponentiation. *IEEE Journal on selected areas in communications*, 11(5):778–784, 1993.

[6] C. H. Lim and P. J. Lee. Security and performance of server-aided RSA computation protocolls. In *Advances in Cryptology - Proceedings of Crypto'95*, volume 963 of *Lecture Notes in Computer Science*, pages 70–83. Springer Verlag, 1995.

[7] T. Matsumoto, H. Imai, C. S. Laih, and S. M. Yen. On verifiable implicit asking protocols for RSA computation. In *Advances in Cryptology - Proceedings of Auscrypt'92*, volume 718 of *Lecture Notes in Computer Science*, pages 296–307. Springer Verlag, 1993.

[8] T. Matsumoto, K. Kato, and H. Imai. Speeding up computation with insecure auxiliary devices. In *Advances in Cryptology - Proceedings of Crypto'88*, volume 403 of *Lecture Notes in Computer Science*, pages 497–506. Springer Verlag, 1989.

[9] V. I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[10] B. Pfitzmann and M. Waidner. Attacks on protocols for server-aided RSA computation. In *Advances in Cryptology - Proceedings of Eurocrypt'92*, volume 658 of *Lecture Notes in Computer Science*, pages 153–162. Springer Verlag, 1993.

[11] J. J. Quisquater and M. De Soete. Speeding up smart card RSA computation with insecure coprocessors. In *Proceedings of Smart Card 2000*, pages 191–197. North Holland, 1991.

[12] H. Ritter. Breaking knapsack cryptosystems by max-norm enumeration. In *Proceddings of 1st International Conference of the Theory and Appications of Cryptology – Pragocrypt'96*, pages 480–492, 1996.

[13] C. P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–191, 1994.

[14] C. P. Schnorr and H. H. Hörner. Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In *Advances in Cryptology - Proceedings of Eurocrypt'95*, volume 921 of *Lecture Notes in Computer Science*, pages 1–12. Springer Verlag, 1995.

[15] V. Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology - Proceedings of Eurocrypt'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer Verlag, 1997.

[16] D. R. Stinson. *Cryptography: Theory and practice.* CRC Press, 1995.

[17] P. van Oorschot and M. Wiener. Improving implementable meet-in-the-middle attacks by orders of magnitude. In *Advances in Cryptology - Proceedings of Crypto'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 229–236. Springer Verlag, 1996.