RSA Key Generation with Verifiable Randomness

Ari Juels[1] and Jorge Guajardo[2]

[1] RSA Laboratories
Bedford, MA, USA
e-mail: ajuels@rsasecurity.com
[2] Department of Electrical Engineering and Information Sciences
Ruhr-Universität Bochum, Germany
e-mail:guajardo@crypto.ruhr-uni-bochum.de

Abstract. We consider the problem of proving that a user has selected and correctly employed a truly random seed in the generation of her RSA key pair. This task is related to the problem of *key validation*, the process whereby a user proves to another party that her key pair has been generated securely. The aim of key validation is to pursuade the verifying party that the user has not intentionally weakened or reused her key or unintentionally made use of bad software. Previous approaches to this problem have been *ad hoc*, aiming to prove that a private key is secure against specific types of attacks, e.g., that an RSA modulus is resistant to elliptic-curve-based factoring attacks. This approach results in a rather unsatisfying laundry list of security tests for keys.
We propose a new approach that we refer to as *key generation with verifiable randomness* (KEGVER). Our aim is to show in zero knowledge that a private key has been generated at random according to a prescribed process, and is therefore likely to benefit from the full strength of the underlying cryptosystem. Our proposal may be viewed as a kind of distributed key generation protocol involving the user and verifying party. Because the resulting private key is held solely by the user, however, we are able to propose a protocol much more practical than conventional distributed key generation. We focus here on a KEGVER protocol for RSA key generation.

Key words: certificate authority, key generation, non-repudiation, public-key infrastructure, verifiable randomness, zero knowledge

1 Introduction

In this paper, we consider the problem of demonstrating that a public key PK is well selected, in other words, that it has been chosen so as to benefit strongly from the security properties of the underlying cryptosystem. This problem has been typically refered to in the literature as that of *key validation*. Interest in key validation arises when a user registers a public key PK of some kind with a

certificate authority (CA) or presents it for use in some other application, such as a group signature scheme. The structure of PK offers only limited assurance about the strength of the corresponding private key SK. For example, in the RSA cryptosystem, it may be that the public modulus n is long, ensuring security against the general number field sieve. At the same time, one of the two component primes may be short, creating vulnerability to elliptic-curve-based factoring attacks. Thus, it is easily possible for a user to generate SK of some weak form so as to render it vulnerable to any of a range of common attacks, without the knowledge of the CA. If SK is, say, a private signing key, then a malicious user of this sort can seek to repudiate transactions based on digital signatures generated using SK, claiming that the vulnerability of SK led to key compromise. The user might, for instance, place an order for a purchase of stock, and then repudiate it if the market subsequently goes down. Weakness in a key may alternatively result because a user has made inappropriate use of the same "stale" key across multiple platforms. For example, a user might choose to make use of the same key for her magazine subscription as for her financial transactions. Finally, and probably most importantly, a weak key may be produced by bad software. Faulty or malicious software might induce a subtle weakness by using a "stale" prime in RSA keys, i.e., using the same component prime in different moduli. As demonstrated by Young and Yung [46], malicious software might create a key that appears to have been correctly generated, but is primed for theft by the creator of the software, a process dubbed "kleptography". A software package may also generate a key that is weak simply because of faulty programming. This last is of perhaps the greatest concern to security architects.

Such concerns and the liability risks they create for certificate issuers have been a recurrent issue in standards bodies for some time, and have thus served as an impetus for investigation into key validation techniques. A key validation protocol aims at enabling a user to prove to a verifying party, with minimal information leakage, that her private key SK has a particular security property that may not be evident from inspection of PK. For example, researchers have proposed protocols enabling the possessor of an RSA private key to prove to a CA with little information leakage that the corresponding public modulus n is the product of two primes p and q of roughly equal length. Such a protocol is included in the appendix to the ANSI X9.31 standard for digital signatures used in financial services applications [2].

Note, however, that an RSA key can also be constructed in such a way that it is vulnerable to any of an arbitrarily long list of special-form factoring algorithms: examples of ones popular in the literature include the so-called $p-1$ attack and $p+1$ attack [34]. These, like many other attacks, are for most purposes regarded as outmoded, given that they are highly unlikely to be feasible if p and q are generated at random according to standard guidelines [40]. An unscrupulous user aiming to weaken her own key, however, need not adhere to any such guidelines, and may well weaken her key relative to some outmoded or even newly devised attack and still claim that her key was compromised. Recognizing that a host of different types of attacks against the RSA cryptosystem are possible, ANSI X9.31

for example includes discussion of a range of key validation tests. It is clear from the outset, though, that this kind of *ad hoc* approach is fundamentally limited: One can always devise a new type of attack and corresponding key validation protocol to add to the list, and no set of litmus tests can guard against use of a stale key.

In this paper, we propose a novel alternative to or enhancement of key validation that we refer to as *key generation with verifiable randomness*, and denote for brevity by KEGVER. A KEGVER protocol shows not that a key is resistant to a list specific attacks, but instead that the key has been generated as an honest party would, and is therefore unlikely to be weak with respect to any known attack and unlikely to be stale. The starting point for our approach may be thought of as an ideal process in which a *trusted dealer* or *trusted third party* (TTP) generates a key pair (SK, PK) according to a universally agreed upon process, e.g., the key generation process outlined in the ANSI X9.31 standard [2], or more broadly by the example methods presented in the IEEE P1363 standard [1]. In this ideal process, the TTP sends (SK, PK) privately to the user and PK to the CA. The user is assured here that the privacy of her key SK is as good as if she had generated it herself. The CA is assured that the key pair (SK, PK) was generated securely, namely according to published guidelines, and therefore benefits from the full strength of the underlying cryptosystem. It should be noted that TTPs form a component of many secret sharing and key distribution schemes, e.g., [42]. The role of the TTPs in these schemes, however, is to effect a correct sharing of secrets. In our ideal process, it is to ensure correct key generation.

Of course, involvement by a TTP in real-world settings is generally undesirable and impractical. It is well known, however, that such a TTP can be simulated by the user and CA alone using fundamental cryptographic techniques known as *general secure function evaluation* [25, 45]. While offering rigorously provable security characteristics, such techniques remain highly impractical, particularly for such computationally intensive operations as key generation. Our contribution in this paper is a technique that simulates the TTP efficiently in a practical sense. The one drawback to our proposal is that it involves a slight weakening of the ideal process: The user is able to influence the TTP to a small (but negligible) degree. We believe that our proposal is of great practical interest, and note that it can even be achieved in a non-interactive setting. We focus primarily on KEGVER protocols for RSA in this paper; the idea is relatively straightforward for discrete-log-based systems, as we show.

A capsule description of our KEGVER protocol for RSA is as follows. The user and CA jointly select random integers x and y; these integers are known to the user, but not the CA. The user then produces an RSA modulus n. She proves to the CA that n is a Blum integer and the product of two primes, p and q. She furthermore proves that p and q lie in intervals $[x, x + l]$ and $[y, y + l]$ for some public parameter l, i.e., that they are "close" to x and y. The parameter l is selected to be small enough to constrain the user in her construction of the modulus n, but large enough to ensure that she can very likely find primes in the

desired intervals. Secure, joint generation of x and y, judicious selection of l, and a number of implementation details form the crux of our work in this paper. As an additional contribution, we propose new definitions required to characterize the security of a KEGVER protocol.

1.1 Previous work

While general secure function evaluation and zero-knowledge proof techniques are largely impractical, researchers have devised a number of efficient protocols to prove specific properties of public keys. One of the earliest such protocols is due to van de Graaf and Peralta [43], who present a practical scheme for proving in zero knowledge that an integer n is of the form $p^r q^s$ for primes p and q such that $p, q \equiv 3 \bmod 4$ and the integers r and s are odd. Boyar *et al.* [8] show how to prove that an integer n is square-free, i.e., is not divisible by the square of any prime factor. Together, these two proof protocols demonstrate that an integer n is a Blum integer, i.e., an RSA modulus that $n = pq$ such that $p, q \equiv 3 \bmod 4$. Gennaro *et al.* [23] build on these two protocols to demonstrate a proof system showing that a number n is the product of quasi-safe primes, i.e., that $n = pq$ such that $(p-1)/2$ and $(q-1)/2$ are prime powers (with some additional, technical properties). Camenisch and Michels [9] extend these proof techniques still further, demonstrating a protocol for proving that an RSA integer is the product of two safe primes, i.e., primes p and q such that $(p-1)/2$ and $(q-1)/2$ are themselves primes. While asymptotically efficient, however, this last protocol is not very practical.

Chan *et al.* [12][1] and Mao [32] provide protocols for showing that an RSA modulus n consists of the product of two primes p and q of large size. Liskov and Silverman [29] describe a protocol interesting for its direct use of number-theoretic properties of n to show that p and q are of nearly equal length. Fujisaki and Okamoto [18, 19] present related protocols for proving in statistical zero knowledge that a committed integer lies within a given range. All of these protocols are largely superseded for practical purposes by the work of Boudot [7], who, under the Strong RSA Assumption, demonstrates highly efficient, statistical zero-knowledge protocols for proving that a committed number lies in a given range. The Boudot protocols permit proofs of very precise statements about the sizes of p and q.

Loosely stated, all of these protocols demonstrate that a committed number (or public key) lies in a particular set or language. Our aim, which may be viewed as complementary, is to show that a committed number has been selected from a given set *at random* according to some publicly specified process. Thus, these previous protocols, and particularly the Boudot protocols, are useful in the construction of our KEGVER scheme. Our focus in this paper, however, is on the additional apparatus required to make broader statements about adherence to a prescribed key-generation protocol.

[1] The original version of this paper contained a technical flaw, and was subsequently republished as a GTE technical report.

A simple approach to ensuring freshness in RSA key generation is for the CA to select a random string s of, say, 100 bits, and require that the leading bits of the public key PK be equal to s. This method, however, has several drawbacks. It only ensures freshness in a narrow sense: While the CA can be assured with high probability that the user has not registered PK before, there is no assurance that the user has not re-used one of the constituent primes of the modulus before. Moreover, by constraining the form of PK, the CA naturally constrains the possible set of private keys SK, leading to some degradation in security. Finally, the required alteration to the key generation process limits compatibility with current prime generation techniques.

A broader but still simple approach proposed for verification of the key generation process is to derive all underlying randomness from application of a pseudo-random number generator to a random initial seed s. This approach has been advocated, for example, as a way of allaying concerns about hidden weaknesses in generation of the public moduli parameters for the DSA [26]; the idea is to derive these moduli from and subsequently to publish s. This approach is similarly adopted in the ANSI X9.31 standard for RSA key generation. The proposal in X9.31 is to generate the key pair from s and to store s along with the private key. In case of dispute about the validity of the key generation process, s can be produced as evidence of good faith key generation. Of course, this approach only provides *ex post facto* arbitration of potential disputes, as revelation of s also discloses the private key.

Distributed key generation is a related area of investigation closer in spirit to our work in this paper. In fact, for discrete-log based cryptosystems, we can use distributed key generation directly to achieve a simple and efficient KEGVER scheme. We sketch the idea here, as it also arises in our construction for RSA. Let $\mathcal{G}$ be a published group of large, known order q over which computation of discrete logarithms is hard. Let g be a published generator for $\mathcal{G}$. The user and CA engage in a distributed key generation algorithm, such as that described in [22]. The output of this process in the two-player case, given at least one honest player, is a public key y with corresponding private key $x \in Z_q$ generated uniformly at random such that $y = g^x$. The user holds share $x_1 \in Z_q$ and the CA holds share $x_2 \in Z_q$ such that $x = x_1 + x_2 \bmod q$. To convert this process into a KEGVER protocol, we have the CA simply send x_2 to the user by way of a private channel.[2] The user can check the correctness of the private key sent by the CA and thereby obtain x. This process ensures two desirable properties of the public key y of the user: (1) The CA is assured that x has been generated uniformly at random; (2) The private key x of the user is as secure against the CA as if the user had generated x by herself. Note that a non-interactive

[2] Of course, creation of a secure private channel here depends on the strength of the random-number generator employed by the user for, e.g., selection of an SSL pre-master secret. If the user has a weak random number generator, however, then no security is possible for her in any case: She can be completely simulated by an adversary. We touch on this issue in section 4.2.

variant of this protocol is possible (with slightly diminished security): The user can simply derive x_2 from $y_1 = g^{x_1}$ using a suitable hash function.

It is possible to adopt the same approach to achieve a KEGVER protocol for RSA. The best basis for this is a distributed key generation protocol presented by Boneh and Franklin [6] and further explored in, e.g., [11, 17, 24, 31, 38]. In this protocol, a minimum of three players (or two, in some variants) jointly generate an RSA modulus n. At the end of this protocol, each of the players holds a share of the corresponding private key. No player learns the whole private key at any point. As for discrete-log based systems, distributed key generation protocol can serve as the basis for a KEGVER protocol for RSA. The idea behind the two-party case is to have the CA act as one player and the user as the other. At the end of the protocol, the CA sends its private key share to the user, who is able then to reconstruct and verify the correctness of the entire private key. This approach enables the CA to be assured that n is generated according to a prescribed protocol, e.g., that p and q are generated uniformly at random from a prescribed range. Likewise, the user in this case can be assured that her private key is not exposed to the CA or to an eavesdropper.

The main drawback to distributed key generation for RSA is that it is quite slow. Malkin *et al.* [31] present experiments involving a highly optimized version of the three-party Boneh and Franklin protocol [6]. These experiments suggest that about 6 minutes of work is required to generate a 1024-bit modulus across the Internet using fast servers. In contrast, convention generation of a 1024-bit RSA on a fast workstation requires less than a second [44]. The basic Boneh and Franklin protocol, moreover, is not secure against active adversaries, and thus would not be suitable by itself as the basis for a KEGVER protocol. Instead, it would be necessary to employ a variant with robustness against malicious players, e.g., [17, 31, 38]. These variants are even less efficient than that of Boneh and Franklin. It is possible to construct a non-interactive KEGVER protocol based on distributed RSA key generation by having the user simulate other players (by analogy with our discrete-log-based example above). The overall costs and complexity of such an approach remain high, however.

Since our aim is not sharing, but rather correct generation of a private key, we adopt an approach in this paper rather different in its technical details from distributed key generation. As a result, we are able to present a KEGVER protocol for RSA that is quite efficient and also has a natural, fully non-interactive variant.

1.2 Our approach

Let us sketch the intuition behind our KEGVER protocol for RSA, expanding on our capsule description in the introduction to the paper. One common technique for generating a component prime of an RSA modulus n is to pick a random starting point r in an appropriate range, and apply a primality test to successive candidate integers greater than r until a (highly probable) prime p is found. This basic approach may be enhanced by means of sieving or other techniques, but is essentially the same in almost all systems in use today. The pivotal idea behind our KEGVER scheme is for the user and CA to generate r jointly in such a

way that r has three properties: (1) r is selected uniformly at random from an appropriate interval; (2) The user knows r; and (3) The CA holds a commitment to r, but does not know r itself. These three requirements are achieved using a protocol much like the KEGVER protocol for discrete log systems sketched above. The user performs the same process to derive a starting point s for a second component prime.

Ideally, we would then like the user to furnish an RSA modulus n and prove that the constituent primes p and q are the smallest primes larger than r and s. In the absence of any known practical technique to accomplish this, we instead adopt a slightly weaker approach. We restrict the user to selection of a modulus n that is a Blum integer, i.e., the product of two primes p and q such that $p, q \equiv 3 \bmod 4$. We use protocols well established in the literature to have the user prove in zero knowledge that n is indeed a Blum integer. We then employ techniques for proofs involving committed integers, and for range proofs in particular. These enable the user to prove in zero knowledge that p is "close" to r and that q is "close" to s.

As a result of this last proof and the fact that r and s are generated jointly, the user is greatly restricted in her choice of p and q. In particular, she must choose each of these primes from a small interval generated uniformly at random. The result is that the user has very little flexibility in her choice of n, and must therefore select a modulus n nearly as strong as if she had adhered honestly to the prescribed key generation protocol. As a tradeoff against the high efficiency of our protocol, a malicious user does in fact have a little "wiggle room" in her choice of n, but this is small for practical purposes. At the same time, use of zero-knowledge (and statistical zero-knowledge) protocols ensures that the CA gains no information about the private key other than that contained in n itself.

Although we do not dilate on the idea in our paper, we note also that KEGVER can also be employed by a user as a local check against "kleptographic" attacks by an RSA key-generation module [46]. For this, the user employs a separate KEGVER module (generated by a separate entity) to check the correct behavior of the key-generation module.

Organization

In section 2, we offer formal definitions for the notion of key generation with verifiable randomness, along with brief description of the cryptographic and conceptual building blocks. We present protocol details in section 3. We offer security and performance analyses in sections 4 and 5 respectively. We provide details on an implementation of KEGVER in section 6.

2 Definitions

Thusfar we have described a KEGVER protocol as one in which the user, through joint computation with a CA, is constrained to produce keys in a manner "close" to honest adherence to some standard key generation algorithm. Our first task is

to characterize formally this notion of "closeness". We assume for the sake of simplicity a cryptosystem in which every public key PK has a unique corresponding private key SK. We refer to a probability d as *overwhelming* in parameter l if for any polynomial *poly* there is some L such that $d > 1 - \frac{1}{|poly(l)|}$ for $l > L$. We let $\in_U$ denote uniform random selection from a set.

We begin by defining key generation and key generation with verifiable randomness. We let keygen denote a key generation algorithm that takes as input a soundness parameter t and a key-size parameter k. With probability overwhelming in t, the algorithm outputs a well-formed private/public key pair (SK, PK). The length of the public key is specified by k: For example, in our RSA-based key generation algorithm, it is convenient to let the output key length be $2k-1$ or $2k$ bits. Let $\mathcal{PK}_k$ denote the set of public keys specified by key-size parameter k, i.e., the set of all such possible outputs PK of keygen. We assume that membership in $\mathcal{PK}_k$ is efficiently computable without knowledge of SK. We let $P_{k,t}$ denote the probability distribution induced by keygen over $\mathcal{PK}_k$ for parameter k, and let $P_{k,t}(PK)$ be the probability associated with key PK in particular.

A KEGVER protocol involves the participation of a user and a CA. The protocol takes as input a key-size parameter k and security parameters l, m, and t. Here, l and t are soundness parameters, while m is a security parameter governing statistical hiding of committed values, as we explain below. If the protocol is successful, the public output of the protocol is a public key $PK \in \mathcal{PK}_k$, and the private output to the user is a corresponding private key SK. Otherwise, the protocol fails, and we represent the public output by $\emptyset$. The probability of protocol failure when the participants are honest is characterized by security parameter l. We let $Q_{k;l,m,t}$ denote the probability distribution induced by output PK over $\mathcal{PK}_k$ by the KEGVER protocol when the two participants are honest. We say that the CA *accepts* if the CA is persuaded that PK has been properly generated; otherwise the CA *rejects* the protocol output.

Definition 1. *Let $Q^A_{k;l,m,t}$ be probability distribution induced by the output of* KEGVER *with fixed key-size parameter k and security parameters l, m and t over executions accepted by an honest CA when the user is represented by an algorithm A (not necessarily honest). We say that* KEGVER *is a* μ-sound KEGVER protocol *for* keygen *if, for any algorithm A with running time polynomial in k, we have*

$$\max_{PK \in \mathcal{P}_k} \frac{Q^A_{k;l,m,t}(PK)}{P_{k,t}(PK)} \leq \mu. \tag{1}$$

□

This definition specifies the soundness of KEGVER, stating that a dishonest user can generate a given key with probability only μ times that of an honest user executing keygen. For small μ, this means that it is infeasible for a dishonest user to persuade the CA to accept the output of the protocol unless its output distribution is similar to that of keygen. Suppose, for example, that keygen is a standard RSA key-generation algorithm for which the RSA assumption [34] is believed to hold. Then if μ is polynomial in k, it is hard for an attacker to weaken

her own key effectively in KEGVER.[3] In particular, we make the following observation; all quantities here are relative to key-size k, while security parameters are fixed.

Observation 1 *Suppose there exist polynomial-time algorithms A and B such that with non-negligible probability, $B(PK) = SK$ for pairs (SK, PK) distributed according to $Q^A_{k;l,m,t}$. If μ is polynomial, it follows that there is a polynomial-time B' such that $B'(PK) = SK$ with non-negligible probability over $P_{k,t}$, and thus that the RSA assumption does not hold on* keygen. □

The other feature we want is for KEGVER is privacy. In particular, we do not want the CA to obtain any (non-negligible) information about SK other than PK. To make this notion more precise, let us consider the following experiment with an adversary A_1. Adversary A_1 engages (not necessarily honestly) in protocol KEGVER with an honest user with parameters k and m. If the protocol is successful, i.e., outputs a public key PK, then A_1 computes and outputs a guess of the corresponding private key SK at the conclusion of the protocol. Let us then consider a second adversary A_2 that is given a public key $PK \in_{Q_{k;l,m,t}} \mathcal{PK}_k$, i.e., a public key drawn from the distribution specified by $Q_{k;l,m,t}$. This adversary likewise computes a guess at the corresponding private key SK, but without the benefit of a transcript from execution of KEGVER.

Definition 2. *We say that* KEGVER *is* private *if for any polynomial-time adversary A_1, there exists a polynomial-time adversary A_2 such that for any polynomial poly there is an L such that $m > L$ implies*

$$\mathsf{pr}[A_1 \textit{ guesses } SK] - \mathsf{pr}[A_2 \textit{ guesses } SK] < 1/|poly(m)|. \tag{2}$$

□

This definition states informally that by participating in protocol KEGVER yielding public key PK, a CA – or an arbitrary eavesdropper – gains only a non-negligible advantage in its ability to compute the private key SK.

Naturally, we can extend this definition to consider an adversary A_1 that engages adaptively in some polynomial number of invocations of KEGVER. As we assume independent randomness for each invocation of the protocols in this paper, however, this extended definition is no stronger for our purposes than Definition 2.

2.1 Building blocks

Throughout most of our scheme, we work over a group $\mathcal{G}$ published by the CA, with order $o(\mathcal{G})$ unknown to the user. We describe $\mathcal{G}$ in the paper as being of

[3] Of course, a malicious user seeking to weaken her own key can tailor an efficient attack algorithm A for factoring n and then promulgate A. For example, A may contain implicit knowledge of one of the component primes of n. The case for repudiation will be difficult to support in such cases, though, as A will be self-indicting.

"unknown order", as contrasted with a group of "known order", i.e., order known to all players. Additionally, the order $o(\mathcal{G})$ must be larger than the maximum value of the target public RSA key n to be generated by the user. For example, if n is to be 1024 bits in length, then $o(\mathcal{G})$ might be 1025 bits in length. Note that if $o(\mathcal{G})$ is small, this may permit the user to cheat, but will not in fact degrade user privacy. Thus it is in the interest of the CA to choose $\mathcal{G}$ with the appropriate order. In our scheme, it is convenient for the group $\mathcal{G}$ to be generated as a large subgroup of Z_N^* for an RSA modulus N with unpublished factorization. All of the protocols described in the paper can be achieved in a group $\mathcal{G}$ of known order, but this results in a substantial degradation in efficiency (although it does eliminate dependence on the Strong RSA Assumption, as explained below).

The CA additionally publishes two generators of $\mathcal{G}$, denoted by g and h. These generators are selected such that $\log_g h$ and $\log_h g$ are unknown to the user. We believe that the best setup for our protocol is one in which the CA lets $N = PQ$, where $P = 2P' + 1$ and $Q = 2Q' + 1$ for primes P' and Q', and selects $\mathcal{G}$ as the cyclic group of order $2P'Q'$, i.e., the groaup of elements with Jacobi symbol 1.[4] The CA would then, e.g., select $g, h \in_U \mathcal{G}$. The CA proves to users that g and h generate the same group. This is accomplished through proofs of knowledge of $\log_g h$ and $\log_h g$, as described below. Since the CA has freedom in selecting N and can therefore manipulate the orders of the groups generated by g and h, however, these proofs of knowledge require t rounds with binary challenges. (This is equivalent to a cut-and-choose proof.) This involves a non-negligible overhead, but the proofs need only be generated by the CA once and checked by each user only upon key registration.

Strong RSA Assumption: Introduced in [18], the Strong RSA Assumption states that does not exist an algorithm A capable of the following in time polynomial in $|N|$. Given an RSA modulus N and a random value $z \in_U Z_N^*$, algorithm A outputs integers u and $e \notin \{-1, 1\}$ such that $z = u^e \bmod N$.

Fujisaki-Okamoto commitment scheme: This commitment scheme, introduced in [18], is essentially a variant on the commitment scheme of Pedersen [36], but adjusted for application to groups $\mathcal{G}$ of unknown order of the form described above. It should be noted that in contrast to the scheme of Pedersen, which is unconditionally hiding, the Fujisaki-Okamoto scheme is only statistically hiding in a security parameter m.

To commit to a value $x \in Z$, the user selects a random commitment factor $w \in_U \{-2^m N + 1, 2^m N - 1\}$. She then computes the commitment $C(x, w) = g^x h^w \bmod N$. For further details on this setup, see [7, 18].

Note that this commitment scheme is only certain to be hiding provided that the CA has selected g and h honestly. In particular, it suffices[5] that $<g>=<h>$.

[4] One must select $\mathcal{G}$ carefully. For example, while certain papers, e.g., [7], state that $\mathcal{G}$ can be any large subgroup of Z_N^*, Mao and Lim [33] provide some caveats on such subgroups with prime order.

[5] In fact, weaker requirements suffice, such as $g \in <h>$ or h having large order in $<g>$. We adhere to the simpler condition $<g>=<h>$ throughout to avoid confusion.

Thus, to ensure secure hiding, we require that the CA prove knowledge of $\log_h g$ and $\log_g h$ over Z_N^*. (Such proofs may be published as non-interactive proofs of knowledge by the CA along with its public parameters.) The Fujisaki-Okamoto commitment scheme is binding assuming the hardness of factoring, i.e., that the user cannot factor N.

Proof of knowledge of discrete log: Suppose that for some $a \in <g>$, a prover wishes to prove knowledge of $x \in Z_N$ such that $y = g^x \bmod N$. The prover may use a variant of the Schnorr proof of knowledge [41] as follows, with soundness parameter t and privacy parameter m. The prover selects $z \in_U [1, 2^m N]$ and computes $w = g^z$. The verifier computes a challenge $c \in_U [0, 2^t - 1]$. The prover returns $r = cx + z$ (over Z). The verifier checks that all elements provided by the prover are in $<g>$. (In our setting, N is a safe prime and $<g>$ is the cyclic group of order $2P'Q'$, as described above, the verifier need merely check that an element has Jacobi symbol 1). Then the verifier checks the equality $g^r = wy^c \bmod N$. The protocol is statistical zero-knowledge provided that $1/2^m$ is negligible. It is sound under the Strong RSA Assumption [18]; without breaking this assumption, a cheating prover is able to succeed with probability at most 2^{-t+1} [9]. This proof of knowledge may be rendered non-interactive if the prover generates the challenge as $c = H(N \parallel g \parallel y \parallel w)$ for an appropriate hash function H. Security may then be demonsrated upon invocation of the random oracle model on H. We assume use of non-interactive proofs in our protocols, and write $POK\{x : y = g^x\}$ to denote a proof of knowledge of the form described here.

Generalized proofs of knowledge of discrete log: As shown in [15, 16], it is possible to construct efficient, general, monotone boolean predicates on statements of knowledge of discrete logs. Efficient proofs across multiple bases are also possible. In [9], it is observed that these general proof techniques may be applied to the setting we describe here involving groups of unknown order. We employ here the notation developed by Camenisch and Stadler [10], in which a proof statement is written in the form $POK\{variables : predicate\}$, where *predicate* is a monotone boolean formula on statements of knowledge of discrete logs, potentially over multiple bases. For example, a proof of equality of two values represented by commitments C_1 and C_2 would be written as follows: $POK\{a, r_1, r_2 : (C_1 = g^a h^{r_1}) \bigwedge (C_2 = g^a h^{r_2})\}$. More recently, Damgård and Fujisaki [39] study a generalization of Fujisaki-Okamoto committments and proofs of knowledge for these, making some minor corrections to [18].

Proofs of secret multiplication: An additional useful tool is proofs of *secret multiplication* [9, 32] in which, for commitments $C_1 = C(d, r_1), C_2 = C(e, r_2)$, and $C_3 = C(f, r_3)$ on d, e, and f respectively, the prover demonstrates that $de = f$ (over Z). In a group of unknown order, this may be accomplished as a proof of the following form: $POK\{d, e, r_1, r_2, r_3 : (C_1 = g^d h^{r_1}) \bigwedge (C_2 = g^e h^{r_2}) \bigwedge (C_3 = C_1^e h^{r_3})\}$. Soundness in this case depends on the Strong RSA Assumption; see, e.g., [18] and [7] for proofs of this form. It is also possible to adapt this protocol

for groups of known order, in which case soundness depends on the discrete log assumption alone. The protocol is much less efficient in this setting, however.[6]

Interval proof: An *interval proof* is a statistical zero-knowledge proof that a committed value lies within some explicitly specified interval. For commitment $C = g^x h^r$, for example, the prover may wish to prove that $x \in [0, 2^{512}]$. Boudot [7] presents two highly efficient interval proof techniques. We consider here the interval proof in [7] *without tolerance*. The goal is for the prover to demonstrate, for explicit integers a and b such that $b > a$ and on commitment C of value x that $x \in [a, b]$. We write $POK\{x, r : (C = g^x h^r) \bigwedge (x \in [a, b])\}$ to represent a proof of this statement.

It is also possible to perform a slightly more efficient interval proof *with tolerance* [7]. An interval proof of this kind demonstrates that $x \in [a - \epsilon, b + \epsilon]$ for some value ϵ, but only guarantees privacy if $x \in [a, b]$. Use of such a proof makes our constructions in this paper slightly more efficient, but is omitted for the sake of conceptual simplicity.

Blum integer proof: As noted above, it is possible to combine the protocols in [8, 43] so as to yield an efficient proof that an integer n is a Blum integer. We denote this proof protocol as applied to n by $\mathsf{Blum}(n)[t]$, where t is a security parameter. If successful, the protocol yields output 'yes', otherwise output 'no'. The protocol can be either interactive or non-interactive. The soundness of the protocol is overwhelming in t, while the computational and communication costs are linear in t.

3 Protocol

We take as our starting point the following algorithm keygen for RSA key generation. We assume that keygen takes as input an even-valued key-size parameter k (essentially half of the modulus length). We also assume the availability of a probabilistic algorithm $\mathsf{primetest}(z, t)$, that takes as input an integer z and soundness parameter t; this algorithm outputs 'yes' if the input element is prime and otherwise, with overwhelming probability in t, outputs 'no'. For technical reasons, our protocol keygen generates RSA moduli n of a special form, namely Blum integers.

Algorithm $\mathsf{keygen}(e, k)[t]$
$r \in_u [2^{k-1}, 2^k - 1]$;
$s \in_u [2^{k-1}, 2^k - 1]$;
while $gcd(e, r - 1) > 1$ or $r \not\equiv 3 \bmod 4$

[6] Roughly stated, when the proof is in a group of known order u with generator g, the prover has the potential to cheat by exploiting the equality $g^x = g^{x+u}$ in addition to her knowledge of u; substantial computational and communications overhead must be devoted to guarding against this. In a group of unknown order, the prover cannot cheat in this way.

or $\mathsf{primetest}[r,t] =$ 'no'
$r \leftarrow r+1$;
while $gcd(e, s-1) > 1$ or $s \not\equiv 3 \bmod 4$
or $\mathsf{primetest}[s,t] =$ 'no'
$s \leftarrow s+1$;
$p \leftarrow r; q \leftarrow s$;
$d \leftarrow e^{-1} \bmod (p-1)(q-1)$;
output $(n = pq, d)$;

The algorithm keygen outputs with overwhelming probability in k and t a Blum integer (and thus RSA modulus) n with a bit length of $2k-1$ or $2k$. Note that for the sake of efficiency, one would generally use a sieving technique in practice to compute p and q. Adoption of sieving would have no impact, however, on the output of the algorithm. Another common practice is to fix a target bit length for n and adjust the intervals for p and q accordingly. We specify keygen as above for simplicity of presentation.

3.1 KEGVER protocol

We are now ready to present the details of our KEGVER protocol for RSA key generation. Prior to execution of the protocol, the CA publishes key-size parameter k and security parameters l, m, and t, along with an RSA modulus N such that $|N| > 2k+1$, and whose factorization it keeps private. The CA additionally publishes g and h of a subgroup $\mathcal{G}$ of Z_N^* such that $|o(\mathcal{G})| > 2k+1$, and a proof $Proof_1 = POK\{a, b : (g^a = h) \bigwedge (h^b = g)\}$. As explained above, the ability of the CA to select N means that the soundness of this proof of knowledge depends upon execution with binary challenges over t rounds.

We begin by introducing a sub-protocol unigen. This protocol enables the user and the CA jointly to select a value $z \in [A, B]$ such that if at least one party is honest, z is distributed across $[A, B]$ uniformly at random. As may be seen from the properties of the building blocks, the soundness of the protocol depends on both the Strong RSA Assumption and the discrete log assumption over $\mathcal{G}$, while privacy is statistical in m. The public output of the protocol is a commitment C_z; the private output, revealed to the user, is z. We let $[A, B]$ denote the input bounds and (n, t) denote the security parameters. We write $(C_z, z) \leftarrow \mathsf{unigen}[A, B](n, t)$ to denote output of public value C_z and private value z from the protocol.

Protocol $\mathsf{unigen}[A, B](m, t)$

1. The user checks the correctness of $Proof_1$, which demonstrates that h and g generate the same group. If $Proof_1$ is incorrect, she aborts.
2. Let $L = B - A + 1$. The user selects $v \in_U [0, L-1]$ and $w_v \in_U [-2^m N, 2^m N]$. She computes $C_v = C(v, w_v)$, and sends C_v to the CA.
3. The CA selects $u \in_U [0, L-1]$ and sends u to the user.
4. The user checks that $u \in [0, L-1]$. If not, she aborts.

5. If $v + u \geq L$, then $o = g^L$; otherwise $o = 0$. The user selects $w_o \in_U [-2^m N, 2^m N]$, computes $C_o = C(o, w_o)$, and sends C_o to the CA.
6. The user executes $Proof_o = POK\{a : h^a = (C_o/g^L) \bigvee (h^a = C_o)\}$. This demonstrates that C_o represents a commitment of g^L or of 0.
7. Let $C_{z'} = C_v g^u / C_o$, a quantity computable by both the user and the CA. The user executes $Proof_{z'} = POK\{a, b : (C_{z'} = g^a h^b) \bigwedge (a \in [0, L-1])\}$. Together, $Proof_o$ and $Proof_{z'}$ demonstrate that $C_{z'}$ represents a commitment of $(u + v) \bmod L$.
8. If the CA is unable to verify either $Proof_o$ or $Proof_{z'}$, then the CA aborts. Otherwise, the public output of the protocol is $C_z = C_{z'} g^A$, and the private output is $z = ((u + v) \bmod L) + A$.

Given unigen as a building block, we are ready to present the full protocol for KEGVER. The basic strategy is for the user and CA to employ unigen to generate r and s, private values from which the user initiates a search for primes p and q. The user then proves, by way of commitments on her private values, that p and q are "close" to r and s respectively, and then that $n = pq$ is a Blum integer. The pair $[e, k]$ is input such that e represents the public exponent and k specifies the bit length of p and q, and thus n. Security parameters are l, m and t. The public output of the protocol is $n = pq$, while the private output is (p, q).

Protocol KEGVER$[e, k](l, m, t)$

1. $(C_r, r) \leftarrow$ unigen$[2^{k-1}, 2^k - 1](m, t)$.
2. $(C_s, s) \leftarrow$ unigen$[2^{k-1}, 2^k - 1](m, t)$. (Note that the expensive verification step 1 in unigen can be omitted here, as it was already executed in the previous invocation.)
3. The user generates a prime $p \geq r$ meeting the conditions: (1) $gcd(e, p-1) = 1$; (2) $p \equiv 3 \bmod 4$; and (3) $p - r$ is minimal. If $p - r > l$, the user aborts, and the protocol output is $\emptyset$.
4. The user generates a prime $q \geq s$ meeting the conditions: (1) $gcd(e, q-1) = 1$; (2) $q \equiv 3 \bmod 4$; and (3) $q - s$ is minimal. If $q - s > l$, the user halts, and the protocol output is $\emptyset$.
5. The user selects $w_p, w_q \in_U [-2^m N, 2^m N]$ and computes $C_p = C(p, w_p)$ and $C_q = C(q, w_q)$.
6. The user sends C_p to the CA and proves $POK\{a, b : (C_p/C_r = g^a h^b) \bigwedge (a \in [0, l])\}$, and analogously for C_q.
7. The user sends $n = pq$ to the CA and proves $POK\{a, b, c, d : (C_p = g^a h^b) \bigwedge (C_q = g^c h^d) \bigwedge (g^n = g^{ac})\}$. In other words, the user proves that C_p and C_q are commitments to factors of n.
8. The user executes Blum$(n)[t]$.
9. If the CA is unable to verify one or more proofs, or if Blum$(n)[t]$ outputs 'no', the CA rejects and the protocol output is $\emptyset$. Otherwise, the public output of the protocol is n and the private output, obtained by the user, is (p, q).

3.2 Non-interactive variant of KEGVER

The protocol KEGVER can be rendered wholly non-interactive by having the user execute all proofs non-interactively and generate the value u in unigen as $H(C_v)$ for an appropriate hash function H. In this case, we really have two algorithms KEGVER_{user} and KEGVER_{CA}, where KEGVER_{user} produces a public key PK and proof transcript T and KEGVER_{CA} decides whether to accept or not to accept a key/transcript pair (PK', T'). To guard against reuse of stale keys, a CA may require that the hash function H be specially keyed in a manner unique to that CA. Of course, this does not prevent intentional subsequent use of stale keys with CAs that do not adopt such a precaution.

Definition 1 must be altered for the non-interactive case. In particular, we define the probability $Q^A_{k;l,m,t}$ so that the probability distribution over keys PK' yielded by polynomial-time attack algorithm A also produces an accompanying transcript T' accepted by the CA. The algorithm A can of course run KEGVER_{user} or some variant algorithm any arbitrary number of times polynomial in k.

4 Security

If $<g>=<h>$, the protocol KEGVER is statistical zero-knowledge with privacy dependent on the parameter m used for the construction of commitments [7, 18]. Details on simulator construction for the CA are available in security proofs for the underlying primitives as presented in the literature. If the proof protocols in KEGVER are to be realized non-interactively (as is better for most practical purposes), then the zero-knowledge property depends additionally on a random oracle assumption on an underlying hash function used for challenge generation [37]. In the case that $<g>\neq<h>$, the commitments of the user may not in fact be statistically secure. Hence, the privacy of KEGVER also depends on the soundness of $Proof_1$. The soundness of all proof protocols depends on the challenge sizes and also, for non-interactive proofs, on the random oracle assumption.

The new and critical security issue we focus on here is the choice of security parameter l and its impact on the soundness bound μ of Definition 1. To address this issue, we require some exploration of number theoretic conjectures regarding the density of primes.

The *prime number theorem* is a well known characterization of the average density of primes, and is as follows [34].

Fact (Prime number theorem): Let $\pi(x)$ represent the number of primes $\leq x$. Then for $x \geq 17$, we have $\pi(x) > \frac{x}{\ln x}$.

This theorem does not specify the likelihood that a given interval contains a prime. A number of researchers, however, have explored the question of maximal gaps between primes. The best, fully proven result to date states that the maximal gap succeeding a prime x is $x^{0.535}$; this is shown by Baker and Harman [3]. For tighter characterizations, we rely on a collection of conjectures, beginning most notably with Cramér [14], who in 1937 conjectured that the maximal gap

between a prime x and the next successive prime is asymptotically $\ll \ln^2 x$. A result by Maier [30] suggests that Cramér's conjecture may be slightly weak, and that $\ll \ln^{2+\epsilon} x$ may be closer to the mark. Empirical investigation has not yielded gaps even close to those suggested by these conjectures. Only recently was a gap of size larger than 1000 discovered, while the largest gap reported to date, by Dubner, is of size 50206 [35]. This gap succeeds a very large prime of size about 3×10^{1883}.

A complementary view of prime density is offered by Gallagher [20], based on an early conjecture of Hardy and Littlewood [27]. Gallagher shows that number of primes in the interval $(x, x + \lambda \ln x]$ is Poisson distributed with mean λ as $x \to \infty$.

The security of our construction depends on a slightly different quantity. In particular, our aim is to find a value l such that for a random k-bit value r, the interval $[r, r + l]$ with overwhelming probability contains a prime p such that $p \equiv 3 \bmod 4$ and $gcd(e, p-1) = 1$. For this, we make two heuristic assumptions. Our first assumption is that the distribution of primes in the range used to construct RSA moduli is roughly Poisson distributed in accordance with the conjecture of Gallagher. We assume, second, that e is an odd prime constant (as is the case in most applications). Finally, let d_1 denote the probability density of primes p of general form; let d_2 denote the probability density of primes p such that $p \equiv 3 \bmod 4$ and $e \not| (p-1)$. We assume, as one would naturally expect, that $d_2/d_1 = (e-1)/2e$. Let X be a Poisson-distributed random variable with mean λ. The probability that $X = 0$ is $e^{-\lambda}$. Thus we obtain the following conjecture.

Conjecture 1. For large r, the probability that the interval $[r, r + l]$ contains no prime $p \equiv 3 \bmod 4$ such that $e \not| (p-1)$ is at most $e^{-\lambda}$ for $l = \lambda \ln r(\frac{2e}{e-1})$ or, equivalently, for $\lambda = \frac{l}{\ln r}(\frac{e-1}{2e})$. □

This conjecture yields the following observation on the best parameterization of λ and l in accordance with Definition 1. It is easy to see that this observation extends to the non-interactive variant of KEGVER.

Observation 2 *Suppose that $\lambda = \omega(\ln \ln r) = \omega(\ln k)$, $t = \omega(\ln k)$ and $\lambda \frac{2e}{e-1} \ln r < l = O(k^c)$ for some constant c. Then the failure probability for an honest user, i.e., the probability that an honest user cannot find suitable primes p and q in* KEGVER *is negligible in k, and the soundness bound μ is polynomial in k.* □

Example 1. Let us consider a concrete example involving the generation of 512-bit primes (and thus roughly a 1024-bit RSA modulus) and public exponent $e = 3$. Choosing $\lambda = 57$ yields a failure probability for an honest user in KEGVER of less than 2^{-80} by Conjecture 1. This corresponds to $l = \lambda \frac{2e}{e-1} \ln r < 60,687$. Clearly, given that at most one in four integers has the form $p \equiv 3 \bmod 4$, the maximum number of primes p in an interval of this size is at most 15,171. It follows then that our KEGVER protocol is μ-sound for $\mu < 15,171^2 = 230,159,241$. This assumes of course that the soundness parameter t is large enough so that the ability of an attacker to cheat in any zero-knowledge proof is negligible, e.g., $t = 100$.

4.1 Stronger concrete security bounds

The concrete security bounds demonstrated in Example 1 above are deceptively weak. First, we note that μ is a bound on the ability of an attacker to distort the output distribution of KEGVER. For this, the ideal strategy is for a malicious user to choose a prime p in the interval $[r, r+l]$ such that the preceding prime p' is as close as possible to p. In fact, though, the aim of a malicious user is entirely different, namely to generate a key that is weak with respect to some attack algorithm or algorithms. Hence, the attacker is much more tightly constrained than our analysis according to Definition 1 suggests at first glance.

Nonetheless, we can achieve substantially stronger concrete security bounds by relaxing Definition 1 in a probabilistic sense across intervals. We do not dilate formally on the idea here. Instead, we note simply that in Example 1 above involving generation of 512-bit primes with $l = 60,687$, the average number of primes of the form $p \equiv 3 \bmod 4$ in the interval $[r, r+l]$ is about 86, and the distribution of such primes is very tightly concentrated around this mean. In fact, under the Gallagher conjecture, the probability that the interval contains more than 250 such primes is well less than 2^{-80}. Thus, given a sufficiently large soundness parameter t (e.g., $t = 100$), the soundness bound $\mu < 250^2 = 62,500$ is a more accurate one for our purposes in Example 1.

Finally, we note that in the interactive case, it is possible to strengthen concrete security bounds by means of the following, simple idea. We select l such that the failure rate of KEGVER is somewhat higher, say, 1 in 1,000,000. When a failure occurs, i.e., when no prime of the right form falls in the interval $[r, r+l]$, the user decommits and the CA checks the user's claim of failure. In particular, the CA checks the fact that there are no primes in the interval. If this is not the case, the CA aborts the protocol; otherwise, the two parties re-initialize KEGVER. In the worst case, the CA will be required for a given invocation of KEGVER to do additional computation roughly equivalent to the generation of an RSA modulus. This will happen, however, only in the case that there is a failure or that the user is malicious, and is thus likely to be a fairly rare occurrence. In non-interactive protocols, transcripts can be seeded by, e.g., the name to be assigned to the certificate along with parameters published by the CA.

4.2 Security model limitations

Thusfar we have considered the security of KEGVER as a two-party protocol involving the user and a CA (or other verifying party). This model is clearly adequate for addressing the problem of key freshness if we assume honest behavior on the part of the CA, who presumably has a vested interest in ensuring against re-use of stale keying material by the user. Our KEGVER protocol also addresses the broader issue of repudiation by assuring the privacy and secure construction of the private key SK of the user. Given honest behavior by the user, the key SK remains safe with high probability even in the face of a potentially malicious CA. As a third party adversary has no better chance of learning SK than the

CA, our two-party model implicitly addresses the possibility of outside attack as well.

A subtle and tacit element of our analysis of KEGVER is the supposition that the user has access to a good random number generator. In particular, we assume that the user is capable of selecting starting points r and s uniformly at random and also capable of selecting secure commitments. One possible means for the user to seek to repudiate a key is to claim that her random number generator was defective, and therefore that the CA was capable of learning and making malicious use of SK. In fact, the problem is broader than this: With poor random number generation, a user cannot establish, e.g., a secure SSL connection to a CA, and can seek to claim compromise by a third party on this basis.

There is no comprehensive technical solution to this problem. If the user has a very poor random number generator whose defects are known to a third party, then that third party can fully simulate the user and compute SK in any setting. Thus, while poor random number generation offers a possible avenue to repudiation, it is not possible to do any better in this sense than our KEGVER proposal here. It should be pointed out, moreover, that random number generation techniques for SSL are standardized and tested on a large set of platforms, so that false claims of weak random number generation by an individual user are generally unlikely to be persuasive.

5 Performance

One of the desirable features of KEGVER is that it places the bulk of the computational burden (primarily in the protocol Blum) on the user, rather than the CA. This preserves the usual balance of computational effort by the two parties. In particular, RSA key generation, which the user must perform in any case, is a computationally intensive task. In contrast, certification of an RSA key by a CA is, in its basic form, a relatively lightweight operation.

We present the computational cost of the protocol in terms of the number of modular exponentiations required by the two parties (disregarding small added costs, such as the fact that Fujisaki-Okamoto commitments require exponents slightly longer than the modulus). Given soundness parameter $t = 100$, the computational requirement for the user in KEGVER is about 35 double exponentiations and 319 single exponentiations. For the CA, it is about 19 triple exponentiations, 2 double exponentiations, and 9 single exponentiations. Assuming use of simultaneous multiple exponentiation, a technique attributed by El Gamal [21] to Shamir, this means the equivalent of about 160 modular exponentiations for the user and about 34 modular exponentiations for the CA. The communication costs are as follows. The transcript sent by the CA to the user, consisting primarily of $Proof_1$, is about 52kB.[7] The size of the transcript sent

[7] This transcript consists almost entirely of $Proof_1$. Recalling that it actually suffices to show $g \in <h>$, we can reduce the size of this transcript to about 26kB and the number of single exponentiations executed by the user to 219.

from the user to the CA is about 38kB. As we now show, we can substantially reduce the computational requirements for the CA.

Batch verification: Our first means of reducing the computational costs of the CA is a method introduced by Chen *et al.* [13] for batch verification of the proofs of knowledge, and pursued in a number of more recent publications, e.g., [4]. The idea is to verify multiple equalities simultaneously by checking their product. The performance of batch verification can often be enhanced substantially by use of addition chains.

Addition chains: Performance here can be improved still further using *addition chains* as recently explored in, e.g., the work of Bleichenbacher [5]. For the task of computing j independent exponentiations, the Bleichenbacher addition chain construction requires computation of M modular multiplications, bounded above as follows:

$$M \leq a + \frac{(j-1)a \ln 2}{\ln(j-1) - \ln\ln(j-1)},$$

where a is the maximum exponent bit length. Using this technique we can reduce the cost of the 19 triple and 2 double exponentiations of the CA to the equivalent of 11 exponentiations. Bleichenbacher reports that computational costs in practice are about a 25% lower than this upper bound. Thus, the cost of the multiple exponentiations for the CA can be reduced to that of slightly more than 8 exponentiations (plus the additional 9 single exponentiations).

Eliminating square-freeness testing: In our computational cost estimate above, the majority (more precisely, 7) of the single exponentiations required by the CA result from the assumption that we invoke 7 rounds of the square-freeness proof protocol of van de Graaf and Peralta [43]. Recall that the protocol in [8] shows that the RSA modulus $n = p^a q^b$ for primes p and q such that $p, q \equiv 3 \bmod 4$ and odd integers a and b such that $a, b \geq 1$. The protocol presented in [43] proves further that $a = b = 1$, i.e., that n is square free. As we shall show, however, the KEGVER protocol itself implicitly enforces the condition of square-freeness with high probability, so that there is no need for explicit proof. In particular, we have the following lemma, whose proof is given in the appendix.

Lemma 1. *Suppose that* $r, s \in_U [2^{k-1}, 2^k - 1]$ *are selected independently, and that* $t < k/3 - 2\log_2 k - \log_2(l+1) - 2$. *Then with probability at least* $1 - 2^{-t}$, *there do not exist values* $u \in [r, r+l]$ *and* $v \in [s, s+l]$ *such that* $n = uv = p^a q^b$ *for primes* p *and* q *and integers* a *and* b *such that* $a \geq 2$ *or* $b \geq 2$. □

Given a typically parameter choice of, for example, $k = 512$ and $l = 60,687$, we have $k/3 - 2 - 2\log k - \log(l+1) > 134$. Therefore, we easily achieve soundness as specified by, e.g., parameter choice $t = 100$.

By eliminating an explicit protocol for having the user prove the square-freeness of n to the CA, we reduce the overall computational cost for the CA

to the equivalent of roughly 10 modular exponentiations. This modification, however, reduces the overall computational cost for the user only slightly, to the equivalent of about 153 modular exponentiations. The transcript size for the full protocol is then about 37kB.

6 Implementation and Results

This section describes an implementation in C of a non-interactive variant of the KEGVER protocol for generation of an RSA modulus of length 1024 to 1025 bits. Timing experiments took place on a Pentium III processor running Windows NT 4.0, with 64 Mbytes of RAM and running at 500 MHz. We compiled our code under gcc version 2.95.3 through use of the UNIX emulation environment Cygwin version 1.3.2. For multiprecision arithmetic, we used the GNU MP library, version 3.1.1. We note that the GMP library computes exponentiations via the sliding-window method for exponentiation [34] which provides roughly a 20–30% speed-up over the binary method for exponentiation. In addition, we implemented routines for double exponentiation using the method of simultaneous multiple exponentiation attributed to Shamir in [21]. Shamir's trick enables the computation of 2 exponentiations at a cost equivalent on average to that 1.25 exponentiations computed via the binary method [34]. Due to time constraints in the construction of the prototype, triple exponentiations were implemented simply through one call each to the double exponentiation and the single exponentiation routines, with multiplication of the partial results. In addition, in all of the computations by the CA (verifier), we employ the Chinese Remainder Theorem (CRT). Table 1 summarizes and compares the timings of five exponentiation operations for a 1026-bit RSA modulus. (See Table 1 for a comparison with other modulus sizes.) Observe that the size of the modulus employed by the CA must be longer than that of the modulus employed by the user. In this table, we let "sim." denote the simultaneous multiple exponentiation method of Shamir.

Exponentiation Type	Avg. Timing (msec)
Single exp. (windowing method)	40.8
Double exp.	80.0
Sim. double exp.	55.7
Sim. double exp. w/ 1 short exp. and CRT	16.9
Sim. triple exp. w/ 1 short exp. and CRT	22.7

Table 1. Exponentiation Timings for 1026-bit arithmetic.

The last two rows of Table 1 provide timings for simultaneous double and triple exponentiation with the use of the CRT where one of the exponents in the

computation is significantly shorter than the modulus. In fact, in all the double and triple exponentiations performed in our protocol by the CA, one of the exponents is the size of the hash function output. This is because the challenges, which in an interactive protocol would be generated by the CA, are generated in the non-interactive version of the protocol by hashing values supplied by the user. In our experiments, the hash function in question is SHA-1, so the output length is 160 bits. Given use of the CRT, the double and triple exponentiations performed by the CA are respectively 1.8 and 2.4 times faster than a single 1026-bit exponentiation. The above timings were obtained by performing 200 executions and computing the average duration for a single one.

Proof/Protocol	# times called	Prover (sec)	Verifier (msec)
unigen	2	2.7	509
rangeproof (long)	(2)	(2.4)	(438)
rangeproof (short)	2	1.7	343
Blum Proof	1	1.3	201
KEGVER	–	10.9	2.05 sec

Table 2. Time Critical Proofs/Protocols in KEGVER

Table 2 summarizes the timings of the critical proofs and protocols in KEGVER. We denote the range proofs by the generic label rangeproof; the label "long" indicates a relatively expensive proof over a large interval, and "short", one on a small interval. The second column in Table 2 indicates the number of times that the specified protocol is called by KEGVER (either user or verifier). There are two calls to unigen; these include two range proofs, whose timings are provided in the next row. (Parentheses indicate that the associated calls and timings are subsumed by calls to unigen.) There are also two independent invocations of short range proofs, one for each of the primes in the RSA modulus. These latter proofs correspond to Step 6 in KEGVER. We observe that roughly 86% of the time required for unigen is in fact accounted for by an invocation of the associated (long) range proofs. Together, invocations of the cryptographic protocols unigen,Blum, and rangeproof (short) account for about 92% of the time required to perform KEGVER, the remainder accounted for by non-cryptographic operations. This is true for both the user and CA.

Differences between protocol and implementation. The following are the major differences between our implementation and the KEGVER protocol described in Section 3:

– We denote range proofs in our table by the generic label rangeproof because we do not in fact employ Boudot proofs as presented in the body of the paper. Instead, we employ an alternative protocol denoted by $\mathsf{SZKrange}^+$ [28].

Appendix B contains a brief description of this protocol. Our reason for employing SZKrange$^+$ regards intellectual-property issues, rather than technical merits. In particular, the SZKrange$^+$ would appear to be free from patent encumbrance, while the Boudot protocol is believed to be the subject of patent applications. It is very important note, however, that the SZKrange$^+$ protocol is about a factor of two slower for our purposes than the Boudot protocol. Thus, substitution of the Boudot protocol for SZKrange$^+$ would immediately yield almost a 50% improvement in the performance of KEGVER (for both the user and CA), since range proofs account for the vast majority of the computation in KEGVER.

- Another important feature of our implementation is the fact that we did not have time to include either batch verification or addition chains. We estimate that these techniques would yield a factor of six improvement in computational efficiency for the CA (on top of that yielded by substitution of the Boudot protocol).
- Table 2 does not include timing measurements for the initial proof of membership performed by the CA (Step 1 in unigen). Since the CA only has to compute this during its parameter generation, this is just a one-time cost.

It is our belief that the execution time of the verifier (i.e., CA) protocol in KEGVER is the critical one in determining the value of KEGVER in a practical setting. For the user, KEGVER would be invoked only rarely as part of a certificate request. Such a request would necessarily be preceeded in any case by a time-consuming RSA key generation operation. Our timings suggest that KEGVER for the user would be roughly equal to the time for this operation, and therefore not encumber the user.

With implemenation of all of the efficiency improvements described above, we believe it possible to achieve roughly a factor of 10 improvement in the performance of the verifier protocol. This would reduce the execution time to about 205 msec, thus, making the protocol efficient and practical.

References

1. IEEE Std. 1363-2000. *Standard Specifications for Public-Key Cryptography.* The Institute of Electrical and Electronics Engineers, 2000.
2. ANSI X9.31 2001. *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (X9.31).* American National Standards Institute (ANSI), 2001.
3. R.C. Baker and G. Harman. The difference between consecutive primes. *Proc. London Math. Soc*, 72(3):261–280, 1996.
4. M. Bellare, J.A. Garay, and T. Rabin. Fast batch verification for modular exponentiation and digital signatures. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT '98*. Springer-Verlag, 1998. LNCS no. 1403.
5. D. Bleichenbacher. Addition chains for large sets, 1999. Unpublished manuscript.
6. D. Boneh and M. Franklin. Efficient generation of shared RSA keys. In B. Kaliski, editor, *Advances in Cryptology – CRYPTO '97*, pages 425–439. Springer-Verlag, 1997. LNCS no. 1294.

7. F. Boudot. Efficient proofs that a committed number lies in an interval. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT '00*, pages 431–444, 2000. LNCS no. 1807.
8. J. Boyar, K. Friedl, and C. Lund. Practical zero-knowledge proofs: Giving hints and using deficiencies. *Journal of Cryptology*, 4(3):185–206, 1991.
9. J. Camenisch and M. Michels. Proving that a number is the product of two safe primes. In J. Stern, editor, *Advances in Cryptology –EUROCRYPT '99*, pages 107–122. Springer-Verlag, 1999. LNCS no. 1592.
10. J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In B. Kaliski, editor, *Advances in Cryptology – CRYPTO '97*, pages 410–424. Springer-Verlag, 1997. LNCS no. 1294.
11. D. Catalano, R. Gennaro, and S. Halevi. Computing inverses over a shared secret modulus. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT '00*, pages 445–452. Springer-Verlag, 2000. LNCS no. 1807.
12. A. Chan, Y. Frankel, and Y. Tsiounis. Easy come - easy go divisible cash. In K. Nyberg, editor, *Advances in Cryptology –EUROCRYPT '98*, pages 561–575. Springer-Verlag, 1998. LNCS no. 1403. Revised version available as GTE tech. report.
13. L. Chen, I. Damgård, and T.P. Pedersen. Parallel divertibility of proofs of knowledge (extended abstract). In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, pages 140–155. Springer-Verlag, 1994. LNCS no. 950.
14. H. Cramér. On the order of magnitude of the difference between prime numbers. *Acta Arithmetica*, 2:23–46, 1937.
15. R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Y.G. Desmedt, editor, *Advances in Cryptology – CRYPTO '94*, pages 174–187. Springer-Verlag, 1994. LNCS no. 839.
16. A. de Santis, G. di Crescenzo, G. Persiano, and M. Yung. On monotone formula closure of SZK. In *35th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 454–465. IEEE Press, 1994.
17. Yair Frankel, Philip D. MacKenzie, and Moti Yung. Robust efficient distributed RSA-key generation. In *Symposium on Principles of Distributed Computing (PODC)*, page 320, 1998.
18. E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In B. Kaliski, editor, *Advances in Cryptology – CRYPTO '97*, pages 16–30. Springer-Verlag, 1997. LNCS no. 1294.
19. E. Fujisaki and T. Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '98*, pages 32–46. Springer-Verlag, 1998.
20. P.X. Gallagher. On the distribution of primes in short intervals. *Mathematika*, 23:4–9, 1976.
21. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.
22. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. The (in)security of distributed key generation in dlog-based cryptosystems. In J. Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, pages 295–310. Springer-Verlag, 1999. LNCS no. 1592.
23. R. Gennaro, D. Micciancio, and T. Rabin. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. In *Proceedings of the Fifth ACM Conference on Computer and Communications Security*, pages 67–72, 1998.

24. N. Gilboa. Two party RSA key generation. In M. Wiener, editor, *Advances in Cryptology – CRYPTO '99*, pages 116–129. Springer-Verlag, 1999. LNCS no. 1666.
25. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *STOC '87*, pages 218–229. ACM Press, 1987.
26. D.M. Gordon. Designing and detecting trapdoors for discrete log cryptosystems. In E.F. Brickell, editor, *Advances in Cryptology – CRYPTO '92*, pages 66–75. Springer-Verlag, 1992. LNCS no. 740.
27. G.H. Hardy and J.E. Littlewood. Some problems on *partitio numerorum* III: On the expression of a number as a sum of primes. *Acta Math.*, 44:1–70, 1923.
28. A. Juels. $\mathsf{SZKrange}^+$: Efficient and accurate range proofs. Technical report, RSA Laboratories, 1999.
29. M. Liskov and B. Silverman. A statistical-limited knowledge proof for secure RSA keys, 1998. Manuscript.
30. H. Maier. Primes in short intervals. *Michigan Math J.*, 32:221–225, 1985.
31. M. Malkin, T. Wu, and D. Boneh. Experimenting with shared generation of RSA keys. In *1999 Symposium on Network and Distributed System Security (SNDSS)*, pages 43–56, 1999.
32. W. Mao. Verifiable partial sharing of integer factors. In *Selected Areas in Cryptography (SAC '98)*. Springer-Verlag, 1998. LNCS no. 1556.
33. W. Mao and C.H. Lim. Cryptanalysis in prime order subgroups of Z_n^*. In K. Ohta and D. Pei, editors, *Advances in Cryptology - ASIACRYPT '98*, pages 214–226. Springer-Verlag, 1998. LNCS no. 1514.
34. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
35. T. R. Nicely and B. Nyman. First occurrence of a prime gap of 1000 or greater, 2001. URL: http://www.trnicely.net/gaps/gaps2.html.
36. T. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91*, pages 129–140. Springer-Verlag, 1991. LNCS no. 576.
37. D. Pointcheval and J. Stern. Security proofs for signature schemes. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, pages 287–398. Springer-Verlag, 1996. LNCS 1070.
38. G. Poupard and J. Stern. Generation of shared RSA keys by two parties. In K. Ohta and D. Pei, editors, *Advances in Cryptology – ASIACRYPT '98*, pages 11–24. Springer-Verlag, 1998. LNCS 1514.
39. I. Damgård and E. Fujisaki. An integer commitment scheme based on groups with hidden order, 2001. IACR eArchive.
40. R. Rivest and B. Silverman. Are 'strong' primes needed for RSA?, 2001. IACR eArchive manuscript.
41. C.P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4:161–174, 1991.
42. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
43. J. van de Graaf and R. Peralta. A simple and secure way to show the validity of your public key. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO '87*, pages 128–134. Springer-Verlag, 1987. LNCS no. 293.
44. M. Wiener. Performance comparison of public-key cryptosystems. *Cryptobytes*, 4(1), 1998.
45. A.C. Yao. Protocols for secure computations (extended abstract). In *FOCS '82*, pages 160–164, 1982.

46. A. Young and M. Yung. Kleptography: Using cryptography against cryptography. In W. Fumy, editor, *Advances in Cryptology - EUROCRYPT '97*, pages 62–74. Springer-Verlag, 1997. LNCS no. 1233.

A Proof of Lemma 1

Lemma 3. *Suppose that* $r, s \in_U [2^{k-1}, 2^k - 1]$ *are selected independently, and that* $t < 2k/3 - 4\log_2 k - \log_2(l+1) - 2$. *Then with probability at least* $1 - 2^{-t}$, *there do not exist values* $u \in [r, r+l]$ *and* $v \in [s, s+l]$ *such that* $n = uv = p^a q^b$ *for primes* p *and* q *and integers* a *and* b *such that* $a \geq 2$ *or* $b \geq 2$.

Proof: $n = uv = p^a q^b$, it is the case that $u = p^{a_1} q^{b_1}$ and $v = p^{a_2} q^{b_2}$ for non-negative integers a_1, a_2, b_1 and b_2 such that $a_1 + a_2 \geq 1$ and $b_1 + b_2 \geq 1$. Let us consider the various ways in which n can contain a square.

Case 1: ($a_i \geq 2$ **and** $b_i = 0$) **or** ($a_i = 0$ **and** $b_i \geq 2$) **for** $i = 1$ **or** $i = 2$

Let us suppose that $u = p^{a_1}$ for $a_1 \geq 2$. This clearly implies $|p| \leq k/2$. The total number of primes of this size is less than $2^{k/2}$, so that the total number of possible k-bit integers of the form p^{a_1} for $a_1 \geq 2$ is less than $2^{k/2}k$. It follows that the probability that an integer of this form lies in $[r, r+l]$ is bounded above by $P_1 = (l+1)2^{k/2}k/2^{k-1} = (l+1)k2^{-k/2+1}$. A similar bound applies to the other three analogous possibilities. Hence the probability that u and v can be selected so as to satisfy Case 1 is at most $4P_1$.

If Case 1 does not hold, then it must be the case that $pq \,|\, u, v$. Otherwise, w.l.o.g., we can assume that $u = p$. Thus $|p| = k$, and hence $v = q$, so that n does not contain a square. This observation yields a classification of the remaining possibilities into the following two cases.

Case 2: $pq \,|\, u, v$ **and** $|p|, |q| \leq k/3$

The total number of primes of length at most $k/4$ bits is bounded above by $2^{k/3}$. Thus, the maximum number of integers of the form required to satisfy this case is $2^{2k/3}k^2$. Hence, the probability that such an integer lies in $[r, r+l]$ is bounded above by $P_2 = (l+1)2^{2k/3}k^2/2^{k-1} = (l+1)k^2 2^{-k/3+1}$. Hence, the probability that u and v can be selected to satisfy Case 2 is bounded above by P_2.

Case 3: $pq \,|\, u, v$ **and** $|p| > k/3$ **or** $|q| > k/3$

Let us consider the possibility that $|p| > k/3$. The total number of prime divisors of length greater than $k/3$ bits for all integers in $[r, r+l]$ is bounded above by $2l$. Call this set of primes Q. The total number of k-bit integers that contain a divisor in Q is $2l2^{2k/3}$. Suppose that r has been selected, and thus Q. If s is now independently chosen, the probability that $[s, s+l]$ contains an integer with a divisor in Q is bounded above by $P_3 = 2(l+1)2^{-k/3+1}$. Hence, the probability that u and v can be selected so as to satisfy Case 3 is bounded above by P_3.

Thus, the probability that n can contain a square is bounded above by $P = 4P_1 + P_2 + P_3$. Assuming $k > 6$, each of P_1, P_2, and P_3 is bounded above by

$(l+1)k^2 2^{-k/3+1}$. It follows that if $t < k/3 - 2\log k - \log(l+1) - 2$, then $P < 2^{-t}$ as desired. □

B SZKrange$^+$

The cornerstone of SZKrange$^+$ as described in [28] is a variant of the Schnorr proof of knowledge adapted for crude range proofs over groups of unknown order. Let us suppose that a prover wishes to prove an upper bound z on the bit-length $|a|$ of an integer a, represented as a basic commitment $C = g^a$. Let k be a soundness parameter, and γ, a statistical privacy parameter. The basic Schnorr-like protocol is as follows:

1. The prover selects $r \in_U \{0,1\}^{\gamma+k+z}$, computes $w = g^r$, and sends w to the verifier.
2. The verifier returns a challenge $c \in_U \{0,1\}^l$.
3. The prover replies with $s = ca + w$ (over $\mathcal{Z}$).
4. The verifier checks that $|s| \leq \gamma + k + z + 1$ and that $g^s = wy^c$.

This procedure, which we call a *SZKrange* (statistical zero-knowledge range) proof, enables the prover to demonstrate not only knowledge of a, but also that $|a| \leq z + \gamma + 2$. In order to achieve statistical security overwhelming in γ, though, the prover will wish to adopt a stricter criterion on a, namely that $|a| \leq z$. Thus the quantity γ may be regarded as a measure of the *inaccuracy* of the proof protocol. A prover that intends to show $|a| \leq z$ can at best show $|a| \leq z + \gamma + 2$. Note that this basic SZKrange proof can be extended to work with Fujisaki-Okamoto commitments on a. We denote such an SZKrange proof here informally by SZKrange$\{C, k, \gamma : [C] \leq z + \{\gamma + 2\}\}$, where $[C]$ denotes the integer represented in the commitment C.

The idea behind SZKrange$^+$ is to reduce the inaccuracy of the basic SZKrange protocol on a Fujisaki-Okamoto commitment C to a at low cost using a pair of simple tricks. The first trick, referred to in [28] as *focusing* is as follows.

1. The prover computes $C' = g^{a^{2^j}} h^{r'}$, a commitment to a^{2^j}, for $2^j > \gamma + 3$.
2. The prover proves in zero knowledge that C' represents a commitment to a^{2^j}, where a is the integer committed to in C. (For this we employ j secret proofs of multiplication in the obvious manner.)
3. The prover proves SZKrange$\{C', k, \gamma : |[C']| \leq z2^j + \{\gamma + 2\}\}$.

This procedure demonstrates that $|[C']| = |a^{2^j}| \leq z2^j + \gamma + 2$, and thus that $|a|2^j \leq z2^j + \gamma + 3$, implying that $|a| \leq z + \frac{\gamma+3}{2^j}$. As a bit length must be integral, and $2^j > \gamma + 3$, this means that $|a| \leq z$. In other words, we obtain a proof of exact bit length with the same security parameters as in SZKrange, but with no inaccuracy. We denote such a proof informally here by SZKrange$'\{C, k, \gamma : |[C]| \leq z\}$. We call 2^j the *degree* of focusing in the proof.

While focusing enables us to prove exact bounds on bit length, it can be computationally expensive when $|a|$ is large. In particular, as computations occur in a group of unknown order, a prover computing $g^{a^{2^j}}$ must work with an exponent of length larger than $|a||\gamma|$. When, say, $|a| = 512$ and $\gamma = 100$ (a choice employed in KEGVER), this involves an exponent of 51200 bits in length.

To reduce the computation required of the prover in cases where $|a|$ is substantially larger than γ, we employ a second trick that is referred to in [28] as *telescoping*. The idea here is to decompose a bitwise into two smaller segments a_1 and a_2. In other words, letting $|$ denote string concatenation, and considering a in bitwise form, we select a_1 and a_2 such that $a = a_2 \,|\, a_1$. Now if we perform an SZKrange$^+$ proof on a_1 with a low degree of focusing and on a_2 with a high degree of focusing, we can obtain an inexpensive range proof with exact accuracy. In particular, letting C again be a Fujisaki-Okamoto commitment to a, the protocol is as follows.

1. The prover computes Fujisaki-Okamoto commitments C_1 and C_2 to a_1 and a_2 respectively, where a_2 is selected such that $|a_2| = \lfloor \gamma/2 \rfloor + 3$.
2. The prover proves in zero knowledge that $a = a_2 \,|\, a_1$. In particular, he proves straightforwardly that $C_2 2^{|a_1|} C_1$ represents a commitment to the same integer as C.
3. The prover proves
   $SZKrange\{C_1, k, \gamma : |[C_1]| \leq z - (\lfloor \gamma/2 \rfloor + 3) + \{\gamma + 2\}\}$.
4. The prover proves
   $SZKrange'\{C_2, k, \gamma : |[C_2]| \leq \lfloor \gamma/2 \rfloor + 3\}$.

This protocol, which we call SZKrange$^+$, proves that $|a| \leq z$. The security parameters are exactly as for SZKrange. The advantage of telescoping here is that for large $|a|$, the protocol SZKrange$^+$ does not involve the long exponentiations required by $SZKrange'$.

In the context of our KEGVER protocol, we find that SZKrange$^+$ requires approximately two times as much computation as the Boudot protocol for $k = \gamma = 100$.