Statistical Zero-Knowledge Proofs from Diophantine Equations*

Helger Lipmaa

Department of Computer Science and Engineering
Helsinki University of Technology
P.O.Box 5400, FIN-02015 Espoo, Finland
helger@tcs.hut.fi

Abstract. We show how to prove in statistical zero-knowledge that a committed integer is nonnegative. Our novel proof system bases on the well-known result of Lagrange that every nonnegative integer is a sum of four squares and on algorithm of Rabin of Shallit that finds such squares efficiently. From this, we derive efficient zero-knowledge proofs for (not) belonging to a finite interval. Our approach can be generalized: Instead of the Lagrangian equation, different Diophantine equations and their Boolean compositions can be used to construct zero-knowledge proofs for belonging to different subsets of integers. Finally, we show how to prove in statistical zero-knowledge that (1) The encrypted value belongs to a range, and (2) The discrete logarithm of the encrypted value belongs to a range.

1 Introduction

We call a zero-knowledge proof system that a committed integer belongs to some set $S \subseteq \mathbb{Z}$ a *range proof (for S)*. Range proofs are important in many applications. For example, in electronic voting protocols a voter often needs to prove in zero-knowledge that she voted for one of the b candidates. For this, one needs a range proof for the set $S = [0, b-1]$. It might also be necessary for the voter to prove in zero-knowledge that her vote was given to a candidate from a certain subset of $[0, b-1]$. Now, the most efficient *statistical* zero-knowledge (SZK) proof system for $S = [a, b]$ was recently proposed by Boudot [Bou00]. Boudot's proof system is communication efficient but has positive (though negligible) completeness error.

In the current paper, we propose a very different range proof for $[0, \infty)$. Our proof system bases on the well known result of Lagrange that every nonnegative integer is a sum of four squares and on the algorithm of Rabin and Shallit that computes these squares efficiently [RS86]. On the other hand, a negative integer cannot be represented as such a sum. With realistic parameters, our proof system requires about 20% more communication than Boudot's proof system but is perfectly complete.

Furthermore, one can use the same methodology as a novel framework to prove that a committed tuple of integers $\mu = (\mu_1, \ldots, \mu_m)$ belongs to any (not necessary finite) set $S \subset \mathbb{Z}^m$:

* Preliminary version, October 25, 2001.

1. Find a small set of sets S_j and polynomials $f_j(x_1, \ldots, x_m, y_1, \ldots, y_n)$, such that (a) Diophantine equation $f_j(x, y) = 0$ has an integral solution $y = (y_1, \ldots, y_n)$ iff $x = (x_1, \ldots, x_m) \in S_j$; (b) For every $\mu = (\mu_1, \ldots, \mu_m) \in S_j$, there is an efficient algorithm to find at least one integral solution $y = (y_1, \ldots, y_n)$ of $f_j(\mu, y) = 0$; and (3) S can be efficiently represented by using the sets S_j and common set-theoretic operations;
2. Prove in statistical zero-knowledge, using an integer commitment scheme, that you know such a solution by using the methodology of [CDS94].

This framework allows to use *any* common set-theoretic operations, including set complementing. For example, we will obtain short SZK proofs that $\mu \in \mathbb{Z} \setminus [a, b]$ for any finite interval $[a, b]$. We will give more details and examples in Section 3.

After that, we turn to the applications. In practice, it is often necessary to show that an *encrypted* (as opposed to a committed) value belongs to an interval. While we are not aware of an *efficient* range proof for $[a, b]$ that would use only the corresponding public-key cryptosystem and no other primitives, we can build up a range proof for encrypted numbers by using a SZK proof that a committed and an encrypted value are equal (modulo the message space size), and then applying our SZK range proof for $[a, b]$ to the committed value. Sequential composition of these two proofs is naturally a SZK proof-of-knowledge. Finally, we construct an efficient SZK proof that discrete logarithm of encrypted value belongs to an interval, and show how to use it in the Damgård-Jurik voting scheme [DJ01] to achieve shorter proofs of vote correctness.

Road-map. Necessary preliminaries are given in Section 2. We will describe our range proof and its extensions in Section 3. Section 4 presents protocols that allow to apply our proofs together with homomorphic cryptosystems.

2 Preliminaries

Homomorphic encryption. Let us recall shortly that a public-key cryptosystem Π is a triple of efficient algorithms, $\Pi = (G, E, D)$, where G is the key generation algorithm, E is the encryption algorithm and D is the decryption algorithm. Throughout this paper, let t be the security parameter. Let $\mathcal{M}$ (resp., $\mathcal{C}$ and $\mathcal{R}$) denote the message space (resp., the ciphertext space and the randomness space), corresponding to t. We assume that all three sets $(\mathcal{M}, \mathcal{R}, \mathcal{C})$ are Abelian groups, with $\mathcal{C}$ written multiplicatively. We say that public-key cryptosystem $\Pi = (G, E, D)$ is *homomorphic* if $E_K(m_1 + m_2; r_1 + r_2) = E_K(m_1; r_1)E_K(m_2; r_2)$. Some example homomorphic cryptosystems are the Paillier cryptosystem [Pai99] and the Damgård-Jurik cryptosystem [DJ01]. Let $M := \lceil \log_2 \sharp\mathcal{M} \rceil$, $C := \lceil \log_2 \sharp\mathcal{C} \rceil$ and $R := \lceil \log_2 \sharp\mathcal{R} \rceil$. We will assume in our calculations that $M = R = 1024$ and $C = 2048$.

Proofs-of-knowledge. For some bit-string α and predicate $P(\cdot)$, $\mathrm{PK}_y(\alpha : y = P(\alpha))$ is a (usually, honest-verifier zero-knowledge) proof-of-knowledge between two parties, that given a publicly known value y, the first party knows a value of α, such that the predicate $P(\alpha)$ is true. To simplify the notation, we will always denote the values,

knowledge of which has to be proven, by Greek letters. Additionally, we assume that the variables denoted by Greek letters are scoped within one proof-of-knowledge. For example, $\mathrm{PK}(c = E_K(m;\rho))$ is a proof that given a ciphertext c, plaintext m and a public key K, the prover knows a nonce ρ such that $c = E_K(m;\rho)$.

Three-round protocols. Most of the protocols in this paper are three-round interactive honest-verifier (statistical) zero-knowledge (abbreviated as HVZK or HVSZK, resp.) proof systems for proofs-of-knowledge of type $\mathrm{PK}(y = P(\alpha))$. One usually proves that such protocols are (1) Complete: That is, a honest verifier accepts a honest prover with probability $1 - \mathrm{neg}(t)$, where $\mathrm{neg}(t)$ is a negligible function in t; (2) Honest-verifier (statistical) zero-knowledge: Even without knowing α, one can generate a view of the protocol that has distribution, indistinguishable from (or statistically close to) the distribution of real views in the case when the verifier is honest; (3) Specially sound: Given two views of the protocol that begin with the same move, but have different second moves, one can compute the secret α. A proof system is called *perfectly complete* if a honest verifier always accepts a honest prover. An honest-verifier (statistical) zero-knowledge proof system can be made noninteractive by using the Fiat-Shamir heuristic [FS86] in the random-oracle model. For this, we introduce a random oracle $H : \{0,1\}^* \to \{0,1\}^{2t}$.

Damgård-Fujisaki integer commitment scheme. A (statistically hiding) integer commitment scheme Com allows a a participant P (a polynomial-time algorithm) to commit to any integer $m \in \mathbb{Z}$, so that (1) For any $m_1, m_2 \in \mathbb{Z}$, the distributions $Com_K(m_1)$ and $Com_K(m_2)$ are statistically close; and (2) It is intractable for P to find another value m_2, such that $Com_K(m_1) = Com_K(m_2)$. On top of that, it is usually required that the integer commitment scheme enables a few proofs-of-knowledge.

The first integer commitment scheme with an efficient zero-knowledge proof-of-knowledge for multiplicative relationship between the committed numbers was proposed by Fujisaki and Okamoto [FO97], but its soundness proof was later found to be flawed. This flaw was corrected by Damgård and Fujisaki, who proposed a new integer commitment scheme in [DF01]. Damgård-Fujisaki integer commitment scheme Com works over a suitable group G. It is assumed, that while the prover knows a reasonably close upper bound $2^B > \mathrm{ord}\, G$ to the order of G, he does *not* know the order itself. Together with group G, a large number F is chosen, such that it is still feasible to factor numbers that are smaller than F. (Say, $F = O(t^{\log t})$. In this paper, we take $F = 2^{80}$.) We refer to [DF01] for the exact definition of "suitable" but remark that G can be chosen as $\mathbb{Z}_n$ for RSA modulus $n = pq$, where $p \equiv q \equiv 3 \pmod 4$, $\gcd(p-1, q-1) = 2$, and the parts of $p-1$, $q-1$ with prime factors less than F are $O(t)$. In this case, $B \leftarrow \lceil \log_2 n \rceil$.

During the setup phase, P and V agree on a group G and integer F. Verifier V chooses a random element $h \in G$, such that $\mathrm{ord}\, h$ is F-rough, and a random $\alpha \in [0, 2^{B+t})$. Let $g = h^\alpha$. V sends the public key $K = (g, h)$ to P and proves in statistical zero-knowledge that $g \in \langle h \rangle$. During commitment to $m \in \mathbb{Z}$, P chooses a random $r \leftarrow [0, 2^{B+t})$ and sends $c \leftarrow g^m h^r$ (that we will denote as $Com_K(m;r)$) to V. To open a commitment, P sends (m, r, b), s.t. $c = g^m h^r b$ and $b^2 = 1$.

Let $\mathcal{C}_{Com}$ denote the commitment space of the used integer commitment scheme and let $C_{Com} := \lceil \log_2 \sharp \mathcal{C}_{Com} \rceil$, with security parameter understood from the context. We will assume in our calculations that $C_{Com} = 1024$.

Proof system for multiplicative relation. For their own integer commitment scheme, Damgård and Fujisaki [DF01] constructed an efficient proof system for $\mathrm{PK}(c_1 = Com_K(\mu_1;\rho_1) \wedge c_2 = Com_K(\mu_2;\rho_2) \wedge c_3 = Com_K(\mu_3;\rho_3) \wedge \mu_3 = \mu_1\mu_2)$ (i.e., for the proof-of-knowledge that the committed value μ_3 is the product of another two committed values). We will next give a brief description of this proof system, assuming that $\mu_i \in [0,T)$ and $\rho_i \in [0, 2^{B+t})$. Let $K = (g,h)$ be the public key.

1. Prover P chooses a random $m_1 \leftarrow_R [0, 2^t FT)$, $r_1 \leftarrow_R [0, 2^{B+2t}F)$, $r_2 \leftarrow_R [0, 2^{B+2t}FT)$ and sends $c_5 \leftarrow g^{m_1}h^{r_1}$, $c_6 \leftarrow c_1^{m_1}h^{r_2}$ to V.
2. Verifier V generates a random $e \leftarrow_R [0,F)$ and sends it to P.
3. Prover sends $m_2 = m_1 + e\mu_2$, $r_3 \leftarrow r_1 + e\rho_2$ and $r_4 \leftarrow r_2 + e(\rho_3 - \mu_2\rho_1)$ to V.
4. Verifier checks that $g^{m_2}h^{r_3}c_2^{-e} = c_5$ and $c_1^{m_2}h^{r_4}c_3^{-e} = c_6$.

Noninteractive version of this proof is (e, m_2, r_3, r_4), with $e = H(c_5, c_6)$, where V verifies that $e = H(g^{m_2}h^{r_3}c_2^{-e}, c_1^{m_2}h^{r_4}c_3^{-e}) \mod 2^t$. With parameters $C_{Com} = 1024$, $F = 2^{80}$, $T = 2^{1024}$, $t = 160$ and $B = 1024$, the noninteractive proof has length $4\log_2 F + 2\log_2 T + 6t + 2B = 320 + 2048 + 480 + 2048 = 4896$ bits or 612 bytes. When $\mu_1 = \mu_2$ (i.e., this protocol is used to prove that μ_3 is a square), one can assume that $\mu_1 = \mu_2 \leq 2^{512}$ and the proof system will be 484 bytes long.

Boudot's range proof for $[0,\infty)$. Boudot's proof system [Bou00] for $\mathrm{PK}(c = Com_K(\mu;\rho) \wedge (\mu \geq 0))$ consists of several steps: First, represent μ as $\mu_1^2 + \mu_2$, where $\mu_1, \mu_2 = \Theta(\sqrt{\mu})$. Since $\mu_1^2 \geq 0$, it is now only necessary to prove that $\mu_2 \geq 0$. Recall that $\mu \leq T$. Second, one can prove that $\mu_2 \geq -\theta$ for $\theta := 2^t FT^{1/2}$ by using the range proof with tolerance by Chan, Frankel and Tsiounis [CFT98]. Now, one has proved that $\mu \geq -\theta$. Fourth, one can achieve zero tolerance by a priori multiplying μ with a suitably chosen constant 2^α such that $\theta < 2^{\alpha/2}$. In this case, $2^{\alpha/2}\mu > -2^{\alpha/2}$ or $\mu_2 > -1$. When suitably modified for Damgård-Fujisaki integer commitment system, this proof system has completeness error $\Theta(1/F)$, and its noninteractive version has length $1166 + \frac{1}{8}\lceil \log_2 T^{1/2} \rceil$ bytes.

3 Range Proofs from Diophantine Equations

3.1 Proof that a Committed Number is Nonnegative

In this subsection, we will give an efficient range proof for $[0,\infty)$, i.e., for $\mathrm{PK}(c = Com_K(\mu;\rho) \wedge (\mu \geq 0))$. In the next subsections we will show how to generalize the given proof system. The next theorem is crucial for our range proof:

Theorem 1. *An integer μ can be represented as $\mu = \mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$ with integer μ_i iff $\mu \geq 0$. Moreover, if $\mu \geq 0$ then the representation $(\mu_1, \mu_2, \mu_3, \mu_4)$ can be computed efficiently.*

Proof. If $\mu \geq 0$, such μ_i exist by a well-known result of Lagrange from 1770. Rabin and Shallit [RS86] proposed a probabilistic polynomial time algorithm for computing the representation. On the other hand, no negative number is a sum of four squares. □

Briefly, during our proof system for $[0, \infty)$, prover first uses the Rabin-Shallit algorithm to represent μ as $\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$. After that, he proves to V in SZK that she knows such a representation. Complete proof system is given by the next theorem:

Theorem 2. *Let Com be the Damgård-Fujisaki integer commitment scheme [DF01], and let $K = (g, h)$ be the public key. (Then $Com_K(m; r) = g^m h^r$.) The following protocol is a perfectly complete, honest-verifier statistically zero-knowledge and specially sound proof system for $\mathrm{PK}(c = Com_K(\sum_{i=1}^4 \mu_i^2; \rho))$, or equivalently in the epistemic sense, for $\mathrm{PK}(c = Com_K(\mu) \wedge \mu \geq 0)$:*

1. *Prover P computes the representation of μ as $\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$, using the Rabin-Shallit algorithm. For $i \in [1, 4]$, P chooses random $\rho_i \leftarrow_R [0, 2^{B+t})$ such that $\sum_i \rho_i = \rho$; P chooses random $m_{1i} \leftarrow_R [0, 2^t F T^{1/2})$, $r_{2i} \leftarrow_R [0, 2^{B+2t} F)$, $r_3 \leftarrow_R [0, 2^{B+2t} F T^{1/2})$, and lets $c_{1i} \leftarrow g^{\mu_i} h^{\rho_i}$, $c_{2i} \leftarrow g^{m_{1i}} h^{r_{2i}}$, $c_3 \leftarrow \prod_i c_{1i}^{m_{1i}} \cdot h^{r_3}$. Prover sends $((c_{1i}, c_{2i})_{i=1}^4, c_3)$ to V.*
2. *V generates a random $e \leftarrow_R [0, F)$ and sends it to P.*
3. *P computes $m_{2i} = m_{1i} + e\mu_i$, $r_{4i} \leftarrow r_{2i} + e\rho_i$, $i \in [1, 4]$, and $r_5 \leftarrow r_3 + e\sum_i (1 - \mu_i)\rho_i$. P sends $((m_{2i}, r_{4i})_{i=1}^4, r_5)$ to V.*
4. *V checks that (a) $g^{m_{2i}} h^{r_{4i}} c_{1i}^{-e} = c_{2i}$ for $i \in [1, 4]$, and (b) $\prod_i c_{1i}^{m_{2i}} \cdot h^{r_5} c^{-e} = c_3$.*

Proof. Completeness: $g^{m_{2i}} h^{r_{4i}} c_{1i}^{-e} = g^{m_{1i} + e\mu_i} h^{r_{2i} + e\rho_i} g^{-e\mu_i} h^{-e\rho_i} = g^{m_{1i}} h^{r_{2i}} = c_{2i}$ and $\prod_i c_{1i}^{m_{2i}} \cdot h^{r_5} c^{-e} = \prod_i c_{1i}^{m_{1i}} \cdot \prod_i (g^{\mu_i} h^{\rho_i})^{e\mu_i} \cdot h^{r_3 + e\sum_i (1-\mu_i)\rho_i} g^{-e\sum_i \mu_i^2} h^{-e\rho} = \prod_i c_{1i}^{m_{1i}} \cdot h^{r_3} = c_3$.

Honest-verifier statistical zero-knowledge. The simulator acts as follows. For $i \in [1, 4]$, generate $c_{1i} \leftarrow_R \mathcal{C}_{Com}$, $m_{2i} \leftarrow_R [0, 2^F T)$, $r_{4i} \leftarrow_R [0, 2^{B+2t} F)$. Generate $e \leftarrow_R [0, F)$, $r_5 \leftarrow_R [0, 2^{B+2t} F T)$. For $i \in [1, 4]$, let $c_{2i} \leftarrow g^{m_{2i}} h^{r_{4i}} c_{1i}^{-e}$. Let $c_3 \leftarrow \prod_i c_{1i}^{m_{2i}} \cdot h^{r_5} c^{-e}$. The resulting view $((c_{1i}, c_{2i})_i, c_3; e; (m_{2i}, r_{4i})_i, r_5)$ is accepting and has distribution, statistically close to the distribution of views in a real execution.

Special soundness (from two accepting views, $((c_{1i}, c_{2i})_i, c_3; e; (m_{2i}, r_{4i})_i, r_5)$ and $((c_{1i}, c_{2i})_i, c_3; e'; (m'_{2i}, r'_{4i})_i, r'_5)$ with $e \neq e'$, one can efficiently find $((\mu_i)_i, \rho)$, such that $c = Com_K(\sum \mu_i^2; \rho)$): Given such views, $g^{m_{2i} - m'_{2i}} h^{r_{4i} - r'_{4i}} = c_{1i}^{e - e'}$, for $i \in [1, 4]$, and $\prod_i c_{1i}^{(m_{2i} - m'_{2i})} \cdot h^{r_5 - r'_5} = c^{e - e'}$. We say that we have a bad case, if either $(e - e') \not| (m_{2i} - m'_{2i})$ or $(e - e') \not| (r_{4i} - r'_{4i})$ for some $i \in [1, 4]$ or $(e - e') \not| (r_5 - r'_5)$ As in [DF01], we can argue that the bad case appears with a negligible probability if the group assumptions hold. Otherwise (when we do not have the bad case), let $\mu_i \leftarrow (m_{2i} - m'_{2i})/(e - e')$ and $\rho_i \leftarrow (r_{4i} - r'_{4i})/(e - e')$; then c_{1i} can be opened as $c_{1i} = g^{\mu_i} h^{\rho_i}$, for $i \in [1, 4]$, and c can be opened as $c = \prod_i c_{1i}^{\mu_i} \cdot h^{(r_5 - r'_5)/(e - e')} = ((g^{\sum_i \mu_i} h^{\sum_i \rho_i})^{\mu_i}) h^{(r_5 - r'_5)/(e - e')} = g^{\sum_i \mu_i^2} h^{\sum_i \mu_i \rho_i + (r_5 - r'_5)/(e - e')}$. □

Noninteractive version of this proof system is $((c_{1i})_i; e; (m_{2i}, r_{4i})_i, r_5)$, where the verifier checks that $e = H((c_{11})_{i=1}^4, (g^{m_{2i}} h^{r_{2i}} c_{1i}^{-e})_{i=1}^4, c^{-e} \prod_i c_{1i}^{m_{2i}} \cdot h^{r_5})$. The length of noninteractive proof system is $4C_{Com} + 2t + 4(B + 3t + 2\log_2 F + \frac{1}{2}\log_2 T) + B + 2t +$

$\log_2 F + \frac{1}{2}\log_2 T = 4096+160+4\cdot(1024+240+160)+1024+160+80+\frac{5}{2}\log_2 T = 11216 + \frac{5}{2}\log_2 T$ bits or $1402 + \frac{5}{16}\log_2 T$ bytes.

Our proposed $[0,\infty)$-range proof is $\approx 20\%$ longer than Boudot's proof system for the same problem. However, our proof system enjoys the property of perfect completeness, while Boudot's proof system has completeness error $\Theta(1/F)$. This result in interesting per se, in particular since no complexity-preserving strong black-box transformation can eliminate completeness error [Vad00].

Overview of the Rabin-Shallit algorithm. For completeness, we will give a short overview of the Rabin-Shallit algorithm [RS86]:

1. Write μ in the form $\mu = 2^s(2k+1)$, where $s, k \geq 0$.
2. If $s = 1$, then
   (a) Choose random $\mu_1, \mu_2 \leq \sqrt{\mu}$, with exactly one of μ_1, μ_2 even. Let $p \leftarrow \mu - \mu_1^2 - \mu_2^2$. Note that $p \equiv 1 \pmod 4$.
   (b) Hoping that p is prime, try to express $p = \mu_3^2 + \mu_4^2$ as follows: First, find a solution u to the equation $u^2 \equiv -1 \pmod p$. (This can be done in various efficient ways; for details see [RS86].) Now compute $\gcd(u+\mathsf{i}, p) = \mu_3 + \mu_4\mathsf{i}$ over the Gaussian integers. Again, this can be done efficiently. Check to see that $p = \mu_3^2 + \mu_4^2$. If not, p was not prime, so go back to step 2a.
   (c) Return $\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$ as a representation.
3. If s is odd but not 1, find a representation for $2(2k+1)$ and then multiply each term by the square t^2, where $t = 2^{(s-1)/2}$.
4. If s is even, find a representation $\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$ for $2(2k+1)$ by step 2. Then convert this to a representation for $(2k+1)$ as follows: Group μ_1, μ_2, μ_3, μ_4 so that $\mu_1 \equiv \mu_2 \pmod 2$ and $\mu_3 \equiv \mu_4 \pmod 2$. Then $(2k+1) = (\frac{1}{2}(\mu_1+\mu_2))^2 + (\frac{1}{2}(\mu_1-\mu_2))^2 + (\frac{1}{2}(\mu_3+\mu_4))^2 + (\frac{1}{2}(\mu_3-\mu_4))^2$. Now multiply by t^2, where $t = 2^{s/2}$.

3.2 General Framework

The ideas used to build the given efficient range proof for $[0,\infty)$ can be generalized to the next proof system for proving that the committed tuple $\mu = (\mu_1, \ldots, \mu_m)$ belongs to some (not necessary finite) set $S \subset \mathbb{Z}^m$:

1. Find polynomials $f_S(x, y)$ with integral coefficients, such that (a) The Diophantine equation $f_S(\mu, y) = 0$ has an integral solution $y = (y_1, \ldots, y_n)$ iff $\mu \in S$; and (b) There is an efficient algorithm that finds at least one such solution $(y_1, \ldots, y_n)$ for each $\mu \in S$;
2. Prove in statistical zero-knowledge by using the methods of Fujisaki and Okamoto [FO97] and integer commitment scheme of Damgård and Fujisaki [DF01], using an integer commitment scheme, that you know such a solution.

A few examples:

1. $f_{[a,\infty)}(x, y_1, y_2, y_3, y_4) = y_1^2 + y_2^2 + y_3^2 + y_4^2 - x + a$ and its complement $f_{[-\infty,b)}(x, y_1, y_2, y_3, y_4) = y_1^2 + y_2^2 + y_3^2 + y_4^2 + x - b$. (Conjectured by Fermat and others, established by Lagrange, 1770. Algorithm by Rabin and Shallit [RS86].)

2. $f_{[0,\infty)\setminus\{4^s(8k+7):s,k\in\mathbb{Z}\}}(x,y_1,y_2,y_3) = y_1^2+y_2^2+y_3^2-x$. (Established by Legendre, 1798. Algorithm by Rabin and Shallit [RS86].)
3. $f_{\mathbb{Z}\setminus\{23,239\}}(x,y_1,\ldots,y_8) = \sum_{i=1}^{8} y_i^3 - x$. (Established by Dickson, 1939. No fast algorithms known.)
4. Linear Diophantine equation $f_{\{(y_1,y_2):\gcd(y_1,y_2)|y_3\}}(x_1,x_2,y_1,y_2,y_3) = y_1x_1 + y_2x_2 - y_3$ has an integral solution exactly if $\gcd(y_1,y_2) \mid y_3$.
5. If $f(x_1,x_2,x_3,y_1,y_2) = y_1^2 - x_1y_2^3 - x_2y_2^2 - x_3$, we can prove in statistical zero-knowledge that we know an integral point on committed elliptic curve.

Due to the lack of general theory of Diophantine equations, there are not many sets S for with readily available functions f_S. However, already existing functions f_{S_i} can be further composed by using Boolean operations (akin to the well-known methodology of Cramer, Damgård and Schoenmakers [CDS94]) to devise proofs-of-knowledge for sets, related to S_i with set-theoretic operations. A concrete example is a range proof of $\mu \in [a,b]$, where one proves that $\mu - a \geq 0$ and $b - \mu \geq 0$. (Note that this proof, $\mathrm{PK}(c = E_K(\mu;\rho) \wedge \mu \in [a,b])$, has length $32804 + \frac{5}{8}\log_2(b-a)$ bytes, since one can set $T \leftarrow b - a$.) This range proof uses a Boolean "and" of two more primitive proofs. Equivalently, prover shows that he knows a solution to a linear Diophantine equation system.

The methodology of [CDS94] only works with monotone Boolean operations: In particular, it is not known, how to derive an efficient proof a committed number is *not* equal to some constant a. (Although such proofs exists [MS97].) An important feature of our proof system is that while still using only monotone Boolean operations, negative range proofs can be implemented efficiently. For example, it is possible to prove that $\mu \notin [a,b]$ by proving that either $\mu - b - 1 \geq 0$ or $a - \mu - 1 \geq 0$. If $a = b$, this yields a statistical zero-knowledge proof that a committed number is not equal to a.

The reason why it is possible to give such efficient proofs lies on the set of "primitive" predicates. Namely, any predicate of form $[\![f(x) = 0]\!]$ can be taken as a basic primitive, where $[\![f(x) = 0]\!]$ means that the Diophantine equation $f(x) = 0$ must have integral solutions. Efficient negative proofs are possible since since of such predicates (like $[\![f_{[0,\infty)(x)=0}]\!]$) specify infinite sets, and their unions have finite complements. Note that proof system for $\mathrm{PK}(c = Com_K(\mu) \wedge \mu \in [a,b])$ basically shows that the prover knows a μ, such that $[\![f_{[a,\infty)}(\mu,y) = 0]\!] \wedge [\![f_{(-\infty,b]}(\mu,y)]\!]$, while proof system for $\mathrm{PK}(c = Com_K(\mu) \wedge \mu \notin [a,b])$ bases on the formula $[\![f_{[b+1,\infty)}(\mu,y)]\!] \vee [\![f_{(-\infty,a-1]}(\mu,y)]\!]$.

As a final example, it is known that some number is prime exactly iff a linear Diophantine equation system of 14 equations and 26 variables has positive integral solutions [Rie94]. Thus, one can prove that a committed number is prime by proving that he knows an integral solution to this equation system, and then proving that all solutions are positive.

4 Applications for Encrypted Numbers

4.1 Proof that committed number = encrypted number

Let (G,E,D) be a homomorphic public-key cryptosystem with $\mathcal{M} = \mathbb{Z}_M$ and public key K_e. In cryptographic protocols, one often needs a zero-knowledge proof that an

encrypted number belongs to some set S. For most of the sets S, we are not aware of any efficient range proofs for $\mathrm{PK}(c = E_{K_e}(\mu;\rho) \wedge \mu \in S)$ that base solely on the security of the used encryption scheme. However, the next methodology enables to give such proof systems, assuming that $S \subseteq \mathbb{Z}_M$ and there is an efficient proof system for $\mathrm{PK}(c = Com_{K_c}(\mu;\rho) \wedge \mu \in S)$, where Com is an integer commitment scheme with key K_c:

1. Prover P creates a random r and sends $c_1 = Com_{K_c}(\mu; r)$ to verifier.
2. Prover P proves to V that $\mathrm{PK}(c = E_{K_e}(\mu;\rho_1) \wedge c_1 = Com_{K_c}(\mu;\rho_2))$.
3. Prover P proves to V that $\mathrm{PK}(c = Com_{K_c}(\mu;\rho) \wedge \mu \in S)$.

Note that $E_{K_e}(m + kM; r) = E_{K_e}(m; r)$ for any $k \in \mathbb{Z}$ and hence the proof in the second step should actually be written as $\mathrm{PK}(c = E_{K_e}(\mu \mod M;\rho_1) \wedge c_1 = Com_{K_c}(\mu;\rho_2))$. However, we will omit $\mod M$ notation for the sake of simplicity.

Assuming that there is an efficient proof system for $\mathrm{PK}(c = Com_{K_c}(\mu;\rho) \wedge \mu \in S)$, we are only left to show the next result.

Theorem 3. *Let Com be an integer commitment scheme and let $\Pi = (G, E, D)$ be a homomorphic public-key cryptosystem. Let $\rho_2 \in [0, 2^{B+t})$. The next proof system presents a complete, honest-verifier statistical zero-knowledge, specially sound proof for $\mathrm{PK}(c_1 = E_{K_e}(\mu;\rho_1) \wedge c_2 = Com_{K_c}(\mu;\rho_2))$, given that $\mu < T$:*

1. *Prover generates $m_1 \leftarrow_R [0, 2^t FT)$, $r_1 \leftarrow_R \mathcal{R}$, $r_2 \leftarrow_R [0, 2^{B+2t}F)$, sets $c_3 \leftarrow E_{K_e}(m_1; r_1)$, $c_4 \leftarrow Com_{K_c}(m_1; r_2)$ and sends (c_3, c_4) to verifier.*
2. *Verifier generates $e \leftarrow_R [0, F)$ and sends e to Prover.*
3. *Prover sets $m_2 \leftarrow m_1 + e\mu$, $r_3 \leftarrow r_1 + e\rho_1$ and $r_4 \leftarrow r_2 + e\rho_2$ and sends (m_2, r_3, r_4) to verifier.*
4. *Verifier checks that $c_3 = E_{K_e}(m_2; r_3) \cdot c_1^{-e}$ and $c_4 = Com_{K_c}(m_2; r_4) \cdot c_2^{-e}$.*

Proof. Completeness. If prover is honest then $E_{K_e}(m_2; r_3) \cdot c_1^{-e} = E_{K_e}(m_2 - e\mu; r_3 - e\rho_1) = E_{K_e}(m_1; r_1) = c_3$ and $Com_{K_c}(m_2; r_4) \cdot c_2^{-e} = Com_{K_c}(m_2 - e\mu; r_4 - e\rho_2) = E_{K_e}(m_1; r_2) = c_4$.

Honest-verifier statistical zero-knowledge. Simulator generates a random quadruple $(e, m_2, r_3, r_4) \leftarrow [0, F) \times [0, 2^t FT) \times \mathcal{R} \times [0, 2^{B+2t})$ and sets $c_3 \leftarrow E_{K_e}(m_2; r_3) \cdot c_1^{-e}$, $c_4 \leftarrow Com_{K_c}(m_2; r_4) \cdot c_2^{-e}$. Clearly, this view is an accepted view. Moreover, it has distribution that is statistically close to the distribution of real view.

Special soundness. Let the next two views be accepting: $(c_3, c_4; e; m_2, r_3, r_4)$ and $(c_3, c_4; e'; m_2', r_3', r_4')$ with $e \neq e'$. We know from [DF01] that then with an overwhelming probability $(e - e') \mid (m_2 - m_2')$. Therefore, $c_2 = Com_{K_c}(\mu;\rho_2)$ with $\mu = \frac{m_2 - m_2'}{e - e'}$. Similarly, $c_1 = E_{K_e}(\mu';\rho_1)$, where $\mu' = \frac{m_2 - m_2'}{e - e'} \mod M$. Hence, $\mu' = \mu \mod M$. □

As previously, let C denote the ciphertext space of Π and C_{Com} the commitment space of Com. Noninteractive version of the presented proof system has length $5t + 2\log_2 F + B + \log_2 T + R = 5 \cdot 80 + 2 \cdot 80 + 1024 + 1024 + 1024 = 3632$ bits or 454 bytes.

Range proof for encrypted number. As a concrete application, let us describe a proof system for $\mathrm{PK}(c = E_K(\mu;\rho) \wedge \mu \in [a,b])$:

1. Prover P generates $r_1 \leftarrow_R [0, 2^{B+2t})$, $c_1 \leftarrow Com_{K_c}(\mu; r_1)$ and sends c_1 to verifier.
2. P proves to V that $\mathrm{PK}(c = E_K(\mu;\rho) \wedge c_1 = Com_{K_c}(\mu;\rho_1))$.
3. P proves to V that $\mathrm{PK}(c_1 = Com_{K_c}(\mu;\rho) \wedge \mu \in [a,b])$.

Noninteractive version of this proof is $C_{Com} + |\mathrm{Committed} = \mathrm{Encrypted}| + |\mathrm{range\ proof}| = 128 + 454 + 2784 + \frac{5}{8}\log_2(b-a) = 3366 + \frac{5}{8}\log_2(b-a)$ bytes long.

As noted before, it must be case that $[a,b] \subset \mathcal{M}$ for this proof to work. In particular, we cannot take $S = [0,\infty)$. Therefore, to construct a proof that an encrypted number μ does not belong to $[a,b] \subset \mathcal{M} = \mathbb{Z}_M$, it does not suffice to prove in step 3 that $\mu \notin [a,b]$: One must prove that $\mu \in [0, a-1] \vee \mu \in [b+1, M-1]$.

4.2 Range proof in exponents for encrypted number

In several cryptographic protocols like electronic voting [DJ01], one needs range proofs in exponents: That is, proofs of type $\mathrm{PK}(c = E_{K_e}(n^\mu;\rho) \wedge \mu \in [a,b])$ for some n. We will give an efficient statistical zero-knowledge proof-of-knowledge of a small discrete logarithm of committed number in the special case when n is prime.

We will first present a proof system for $\mathrm{PK}(c = Com_K(m;\rho))$:

1. Prover P generates a $r_1 \leftarrow_R [0, 2^{B+2t}F)$ and sends $c_1 \leftarrow Com_K(m; r_1)$ to V.
2. Verifier V sends $e \leftarrow_R [0, F)$ to P.
3. Prover sends $r_2 \leftarrow r_1 + e\rho$ to V.
4. Verifier checks that $c_1 = Com_K(m; r_2) \cdot c^{-e}$.

Noninteractive version of this proof system is $(e; r_2)$, where the verifier has to check that $e = H(Com_K(m;r_2)\cdot c^{-e}) \mod 2^t$. Length of this proof system is $\log_2 F + B + 4t = 80 + 1024 + 4 \cdot 80 = 1424$ bits or 178 bytes.

As before, it is sufficient to give a proof system for $\mathrm{PK}(c = E_{K_e}(n^\mu;\rho) \wedge \mu \in [0,b])$. Since n is a prime, $\log_n m \in [0,b]$ iff $m \mid n^b$ and $\mu > 0$. Using this observation and ideas from the previous sections of the current paper, we have established that one needs to prove that $\mathrm{PK}(c = E_{K_e}(\mu;\rho) \wedge c_2 = Com_{K_c}(\mu;\rho_2) \wedge c_3 = Com_{K_c}(\mu_3;\rho_3) \wedge c_4 = Com_{K_c}(n^b;\rho_4) \wedge \mu\mu_3 = n^b \wedge \mu > 0)$:

1. Prover generates $r_1 \leftarrow_R [0, 2^{B+2t})$, $c_2 \leftarrow Com_{K_c}(\mu; r_1)$, $r_2 \leftarrow_R [0, 2^{B+2t})$, $r_3 \leftarrow_R [0, 2^{B+2t})$, $c_3 \leftarrow Com_{K_c}(n^b/\mu; r_2)$, $c_4 \leftarrow Com_{K_c}(\mu_4; r_3)$. She sends (c_2, c_3, c_4) to verifier.
2. P proves to V that $\mathrm{PK}(c = E_{K_e}(\mu;\rho_1) \wedge c_2 = Com_{K_c}(\mu;\rho_2))$.
3. P proves to V that $\mathrm{PK}(c_4 = Com_{K_c}(n^b;\rho))$.
4. Prover P proves to V that $\mathrm{PK}(c_4 = E_{K_e}(\mu_4;\rho_4) \wedge c_3 = E_{K_e}(\mu_3;\rho_3) \wedge c_2 = E_{K_e}(\mu_2;\rho_2) \wedge (\mu_4 = \mu_3\mu_2))$.
5. P proves to V that $\mathrm{PK}(c_2 = E_{K_e}(\mu;\rho) \wedge \mu \geqslant 0)$.

Noninteractive version of this proof system has length $384 + 454 + 178 + 602 + 1402 + \frac{5}{16}\log_2(b-a) = 3020 + \frac{5}{16}\log_2(b-a)$ bytes. As an interesting sidenote, one could further shorten this proof by using the result of Legendre that if $n^\mu \neq 4^s(8k+7)$ for some s, k (for example, if n is a power of two) then n^μ can be represented as a sum of three squares.

Application to E-voting. Until now, the best (perfect) zero-knowledge proof system for the same problem seems to be due Damgård and Jurik [DJ01]. While their range proof in exponents does not require n to be a prime, its length is $\approx \lceil \log_2 V \rceil \cdot (6C + M + 3t + 4R)$, where V is the number of candidates to vote for. In their proof system, the length of the interaction is greater than in ours as soon as $V \geq 8$.

Acknowledgments and Further Work

We would like to thank Jeffrey Shallit and Petteri Kaski for useful discussions. In particular, the given description of the Rabin-Shallit algorithm is from [Sha01].

It seems that efficient range proofs can be given for many interesting sets $S \subset \mathbb{Z}$. We did certainly not mention all cryptographically relevant sets S for which efficient proof systems can be constructed by using the current state of knowledge in Diophantine analysis. For even more sets, such proofs systems will become available with the advance of methods in Diophantine analysis. Moreover, it is not known how to generalize Rabin-Shallit algorithm efficiently to higher than the second power.

References

[Bou00] Fabrice Boudot. Efficient Proofs that a Committed Number Lies in an Interval. In Bart Preneel, editor, *Advances on Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 431–444, Bruges, Belgium, 14–18 May 2000. Springer-Verlag.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo G. Desmedt, editor, *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187, Santa Barbara, USA, 21–25 August 1994. Springer-Verlag.

[CFT98] Agnes Chan, Yair Frankel, and Yiannis Tsiounis. Easy Come - Easy Go Divisible Cash. In Kaisa Nyberg, editor, *Advances on Cryptology — EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 561–575, Helsinki, Finland, June 1998. Springer-Verlag.

[DF01] Ivan Damgård and Eiichiro Fujisaki. An Integer Commitment Scheme Based on Groups with Hidden Order. Technical Report 064, IACR, 13 August 2001. Available from `http://eprint.iacr.org/2001/064/`.

[DJ01] Ivan Damgård and Mads Jurik. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In Kwangjo Kim, editor, *Public Key Cryptography '2001*, volume 1992 of *Lecture Notes in Computer Science*, pages 119–136, Cheju Island, Korea, 13–15 February 2001. Springer-Verlag. ISBN 3-540-41658-7.

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations. In Burton S. Kaliski, editor, *Advances on Cryptology — CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 16–30, Santa Barbara, USA, 17–21 August 1997. Springer-Verlag. ISBN 3-540-63384-7.

[FS86] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology—CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer-Verlag, 1987, 11–15 August 1986.

[MS97] Markus Michels and Markus Stadler. Efficient Convertible Undeniable Signature Schemes. In *Proc. 4th Workshop on Selected Areas in Cryptography (SAC'97)*, pages 231–244, Ottawa, Canada, 1997.

[Pai99] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Jacques Stern, editor, *Advances on Cryptology — EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, Prague, Czech Republic, 2–6 May 1999. Springer-Verlag.

[Rie94] Hans Riesel. *Prime Number and Computer Methods for Factorization*, volume 126 of *Progress in Mathematics*. Birkhäuser, 1994. 2nd edition.

[RS86] Michael O. Rabin and Jeffrey O. Shallit. Randomized Algorithms in Number Theory. *Communications in Pure and Applied Mathematics*, 39:239–256, 1986.

[Sha01] Jeffrey O. Shallit. Personal communication, October 2001.

[Vad00] Salil P. Vadhan. On Transformation of Interactive Proofs that Preserve the Prover's Complexity. In *Proceedings of the Thirty-Second Annual ACM Symposium on the Theory of Computing*, pages 200–207, Portland, Oregon, USA, 21–23 May 2000. ACM.