# Cryptography in an Unbounded Computational Model

David P. Woodruff[1] and Marten van Dijk[1,2]

[1] MIT Laboratories for Computer Science, Cambridge, USA
dpwood@mit.edu, marten@caa.lcs.mit.edu
[2] Philips Research Laboratories, Eindhoven, The Netherlands

**Abstract.** We investigate the possibility of cryptographic primitives over nonclassical computational models. We replace the traditional finite field $F_n^*$ with the infinite field $\mathbb{Q}$ of rational numbers, and we give all parties unbounded computational power. We also give parties the ability to sample random real numbers. We determine that secure signature schemes and secure encryption schemes do not exist. We then prove more generally that it is impossible for two parties to agree upon a shared secret in this model. This rules out many other cryptographic primitives, such as Diffie-Hellman key exchange, oblivious transfer and interactive encryption.

## 1 Introduction

In the classical model of cryptography, parties represent data as a sequence of bits, and have a small set of bit operations to work with. Usually some parties are restricted to a polynomial number of operations in the size of a security parameter. In our model, all parties start with the field of rational numbers $\mathbb{Q}$, and have a certain set of operations to work with. We will consider the standard sets of field operations {+, -, *, /}. We give all parties the ability to sample a uniform distribution of real numbers over a bounded interval. Furthermore, all parties have unbounded computational power; that is to say, all parties can perform any finite number of field operations.

It is critical that we give all parties the ability to sample from a uniform distribution of real numbers so that they can generate random secrets that are unpredictable to an adversary. Otherwise any "secret" used by one party could be generated by another party. Indeed, the rational numbers are countable. Therefore, any adversary could simply enumerate elements of his field until he encounters another party's secret since he has unbounded computational time. When we allow sampling from the reals, we are allowing parties to sample from an uncountable domain. Therefore, an adversary cannot simply enumerate the elements of his field to find another party's secret.

The existence of many cryptographic primitives, such as signature schemes, encryption schemes, and identification protocols, depends on the existence of one-way functions and trapdoor functions. In [5] Rompel shows that one-way functions are necessary and sufficient for secure signature schemes to exist in the standard computational model. The proof relies on the bit-representation of numbers in the number field the parties are working in. In our model, bit-representations play no role. Parties are equipped with infinite-precision registers with the ability to perform any field operation on irrational numbers in constant time.

We do not need to speculate about the existence of one-way functions in this model. Over the rational numbers, a party can sample a random real number $r$ and publish its square $r^2$. It is impossible to deduce $r$ to infinite precision from $r^2$ and $\mathbb{Q}$ using only the operations $\{+, -, *, /\}$. Even if one were to sample real numbers, there are only a countable number of real numbers that could help one deduce $r$ from $\mathbb{Q}(r^2)$, but we're drawing from an uncountable set. Hence, there is zero probability of deducing $r$ from $r^2$ and $\mathbb{Q}$, so the function $f(r) \rightarrow r^2$, where $r$ is a real number, is a one-way function in this model.

Given that we have one-way functions, it is only natural to ask which cryptographic primitives are possible. In [2], an elegant proof of knowledge was presented over the ruler-compass constructible points, and then extended to an authentication protocol. What, if any other, primitives are possible over the ruler-compass constructible points? In our model, we will see that authentication protocols exist but secure signatures schemes and public-key encryption schemes do not. We conjecture the same to be true of the ruler-compass constructible points.

Secion 2 covers some standard techniques in modern algebra, focusing mainly on the theory of field extensions. The theorems presented in this section are crucial to understanding the impossibility proofs in the remaining sections. Section 3 presents an authentication protocol in this model. Section 4 shows that secure encryption schemes do not exist and section 5 shows the same for secure signature schemes. Finally, Section 6 shows more generally that it is impossible to share a secret in this model.

## 2 Algebraic Preliminaries

The proof of knowledge presented in [2] over the ruler-compass constructible points is based on the idea that trisecting an arbitrary angle is impossible with only a ruler and a compass. Although it is well-known that one cannot trisect an arbitrary angle, the proof is not well-known. Proving that signature schemes and encryption schemes are not possible over the rationals requires field-theoretic techniques similar to those used in [1] where angle trisection is shown to be impossible. We state and develop some of these techniques here. We assume familiarity with the definition of a field. We shall restrict our attention to infinite subfields of the real numbers.

A real number $x$ is said to be *algebraic* over a field $F$ if $x$ is a root of a polynomial $p(t)$, with coefficients in $F$ in the indeterminate $t$. If no such polynomial exists, $x$ is said to be *transcendental* over $F$. For example, $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it satisfies the polynomial $p(t) = t^2 - 2$. We can think of a transcendental element over a field $F$ as a "variable" over that field. For example, the symbol "$y$" and the number $\pi$ are transcendental over $\mathbb{Q}$ because they do not satisfy a polynomial $p(t)$ with rational coefficients [4]. A new field can be obtained by taking the set-theoretic union of the elements of $F$ with $x$, then closing up under all of the field operations {+, -, *, /}. This new field, denoted $F(x)$, is the minimal field containing $F$ and $x$, i.e., the intersection of all fields containing $F$ and $x$.

The new field $F(x)$ can be thought of as a vector space over $F$. A *basis* for this vector space is a set of elements $\{v_\alpha\}$ such that every element of $F(x)$ can be written as a unique finite linear combination of the form $f_1 v_{\alpha_1} + f_2 v_{\alpha_2} + ... + f_n v_{\alpha_n}$, where $f_i \in F$ for all $i$. The dimension of this vector space is defined as the number of elements in any basis. If $x$ is algebraic over $F$, then there exists a polynomial $q(t)$ of minimal degree such that $q(x) = 0$. It is a theorem of algebra [3] that, if $x$ is algebraic over $F$ and $q(t)$ denotes its minimal polynomial over $F$, then the set $\{1, x, x^2, x^3, ..., x^{(n-1)}\}$ forms a basis for the extension field $F(x)$ viewed as a vector space over $F$, where $n$ is the degree of $q(t)$. Hence, the dimension of this vector space is equal to the degree of $q(t)$. Call this degree the degree of the *field extension* $F(x)/F$ and denote it by $[F(x) : F]$. If $x$ is transcendental over $F$, then there is no finite basis of $F(x)$ over $F$. In this case $[F(x) : F] = \infty$. Furthermore, the elements of $F(x)$ constitute the set of all elements of the form $p(x)/q(x)$, $q(x) \neq 0$, where $p$ and $q$ are polynomials with coefficients in $F$ in the indeterminate $x$.

More generally, any field extension $K/F$ can be viewed as a vector space over $F$. The degree $[K : F]$ of this extension denotes the (possibly infinite) number of elements in any basis of $K/F$. It is a well-known fact that if we have the field inclusions $F \subset L \subset K$, then the degree $[K : F]$ of the extension $K/F$ is equal to the product of the degrees $[K : L]$ and $[L : F]$. We will use this fact frequently and refer to it as the *Tower Law*. For example, since $\sqrt{2}$ is irrational, it does not lie in $\mathbb{Q}$. It satisfies the polynomial $p(t) = t^2 - 2$. Clearly, $p(t)$ is the polynomial of minimal degree of $\sqrt{2}$ over $\mathbb{Q}$, as otherwise there would be a polynomial $q(t) = q_1 t + q_2$, such that $q(\sqrt{2}) = q_1\sqrt{2} + q_2 = 0$, implying $\sqrt{2} = -q_2/q_1$ and therefore that $\sqrt{2}$ is rational. Hence, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. It is not hard to see that $\sqrt{3}$ is not in the field $\mathbb{Q}(\sqrt{2})$ (indeed, $\sqrt{3} \neq q_1 + q_2\sqrt{2}$ for any $q_1, q_2$ in $\mathbb{Q}$). Since $\sqrt{3}$ satisfies the polynomial $p(t) = t^2 - 3$ over $\mathbb{Q}$, it also satisfies this polynomial over $\mathbb{Q}(\sqrt{2})$, and since it is not contained in $\mathbb{Q}(\sqrt{2})$, this polynomial has minimal degree. Hence, we have the field inclusions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, so by the Tower Law $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. A basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Also note that if $[K : F] = 1$, then $K = F$. Indeed, $[K : F] = 1$ implies that there is only one element in any basis of $K$ over $F$. Consider the set $\{1\}$, where 1 is the identity element of $F$. Trivially, this is a linearly independent set, and since we know the size of any basis is one, $\{1\}$ also spans $K$ over $F$, so $\{1\}$ is a basis. Any element of $K$ can be written as $f \cdot 1$, for $f \in F$. This implies $K = F$.

Given a field extension $F(x)/F$, we can adjoin another element $y$ to the field $F(x)$, obtaining the field $F(x)(y)$. It is a standard fact that $F(x)(y) = F(y)(x)$. We will let $F(x, y) = F(x)(y) = F(y)(x)$.

We now define the *algebraic closure* of a field. Consider an infinite field $F$. Consider the set $S$ of all polynomials $p(t)$ with coefficients in $F$ in the indeterminate $t$. Suppose we take the minimal field containing $F$ and adjoin all the roots of all the polynomials of $S$. This new field will be called the algebraic closure of $F$. For the countably infinite fields we shall be dealing with, it is known [4] that the cardinality of the algebraic closure of $F$ is also countable.

We will need some specific facts concerning transcendental field extensions. Let $x$ be transcendental over a field $F$ and let $K = F(x)$. Then any element $u \in K$ can be written as $p(x)/q(x)$, where $p$ and $q$ are relatively prime polynomials with coefficients in $F$ in the indeterminate $x$. We have that $F(u) \subset K$. In [4] it is shown that the degree $[K : F(u)]$ equals $max\{deg(p(x)), deg(q(x))\}$.

We will also need some specific results concerning the intermediate fields of a field extension. A field $L$ such that $F \subset L \subset K$ is called an intermediate field of the field extension $K/F$. If $x$ is transcendental over $K$, it is clearly transcendental over $F$ since $F \subset K$. Conversely, if every element $k \in K$ is algebraic over $F$ and if $x$ is transcendental over $F$, it is also transcendental over $K$. This follows from the transitivity property of being algebraic, namely, if $x$ is algebraic over $K$, and $K$ is algebraic over $F$, then $x$ is algebraic over $F$ [4].

Suppose $x$ is transcendental over $F$, and $K$ is an algebraic extension of $F$, then the intermediate fields $L$ of $K/F$ are in bijective correspondence with the intermediate fields of $K(x)/F(x)$. The bijection sends an intermediate field $L$ of $K/F$ to the intermediate field $L(x)$ of $K(x)/F(x)$. The inverse sends an intermediate field $G$ of $K(x)/F(x)$ to $G \cap K$. The intuition behind this fact is that $x$, being transcendental over $F$, plays no role in factoring the minimal polynomials of elements of $K$ over $F$. Since the intermediate fields of $K(x)/F(x)$ are determined by these polynomials, the intermediate fields of $K(x)/F(x)$ are exactly those of $K/F$ with the additional element $x$ adjoined. This result also holds if $K$ is a transcendental extension of $F$ and $x$ is transcendental over $K$. See [4] for more details.

The final theorem that we will need, due to Lüroth [4], states that if $x$ is transcendental over a field $F$, then the intermediate fields $L$ of the field extension $F(x)/F$ all have the form $F(u)$, where $u$ has the form $p(x)/q(x)$, where $p$ and $q$ are polynomials with coefficients in $F$ and $q \neq 0$.

## 3 An Identification Protocol

Here is a simple zero-knowledge proof of knowledge similar to that in [2]. Suppose Alice wishes to identify herself to Bob. She samples a random real number $r$ and publishes $p = r^2$. Because finding the exact square root of $r^2$ over $\mathbb{Q}$ with only the operations {+, -, *, /} is impossible, Alice knows she is the only one who knows $r$. Also, even if parties are allowed to sample random real numbers, the probability is zero that any number sampled will help an adversary compute $r$ from $\mathbb{Q}$ and $r^2$. Here's the protocol:

1. Alice samples a real number $s$. She gives Bob $t = s^2$.
2. Bob flips a coin and tells Alice the result.
3. – If Bob said "heads", then Alice gives Bob $s$, and Bob checks that $s^2 = t$.
   – If Bob said "tails", then Alice gives Bob $u = rs$, and Bob checks that $u^2 = pt$.

We sketch a proof of the three properties of zero-knowledge: completeness, soundness, and zero-knowledge. For completeness, note that if Alice and Bob follow the protocol, then Bob always accepts Alice's proof of identity. For soundness, note that anyone impersonating Alice cannot respond to both of Bob's challenges because he cannot know both $s$ and $rs$, as otherwise he could compute $(rs)/s = r$, contradicting the fact that it is not possible to compute $r$ given only $\mathbb{Q}$ and $r^2$ in our model of computation. Hence, with each iteration of the above protocol an impersonator can succeed with probability at most $1/2$. After $k$ iterations, the probability that Bob will be fooled by the impersonator is at most $2^{-k}$.

To show the protocol is zero-knowledge, we construct a simulator to produce transcripts of Bob's view in the protocol. Bob's views are of the form $(t, \text{“heads”}, s)$ or $(t, \text{“tails”}, u)$. The first can be simulated by choosing s at random and setting $t$ to be $s^2$. The second can be simulated by choosing $u$ at random and taking $t$ to be $u^2/p$. As stated in [2], even if Bob is to use a nonuniform distribution, his view can be simulated by probing and resetting him. If $k$ rounds are executed in series, the expected number of trials of the simulator is $2k$. If $k$ flips are sent in parallel, then the expected number of trials is $2^k$; this is not a problem since there are no complexity assumptions in our computational model.

## 4 The Impossibility of Secure Public-Key Encryption Schemes

We now address the possibility of secure encryption schemes in this model. We would like an encrypter to be able to encrypt an arbitrary real number of his choice, even after the public and secret keys have been generated. Intuitively, such encryption schemes cannot exist because both the message space and the ciphertext space are uncountably infinite, whereas the set of numbers that are "algebraically dependent" on any finite set of secret keys is only countably infinite. Since all parties are restricted to finite time, only a finite set of secret keys can be generated. Hence, the trapdoor information that comes with knowledge of the set of secret keys can only help decrypt a countable number of messages. We now formalize this intuition.

We first consider a special scenario. Suppose Alice starts with the field $\mathbb{Q}$. She then samples a random real number $SK$ to be her secret key. She now has the field $\mathbb{Q}(SK)$. Suppose she then performs some finite number of field operations in the field $\mathbb{Q}(SK)$ to compute her public key $PK$, another element of $\mathbb{Q}(SK)$. She then publishes $PK$. We first consider the case when the degree $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ is finite.

We would like Bob to be able to encrypt an arbitrary real number $m$ using Alice's public key $PK$, generating a ciphertext $c$. Given the ciphertext $c$ and $PK$, we do not want an adversary to be able to decrypt $c$ to obtain the original message $m$. However, we do want Alice to be able to use her secret key $SK$, together with $c$, to decrypt $c$ and recover the original message $m$. Collecting this information, we have the following tower of fields:

$$\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m) \subset \mathbb{Q}(SK, c).$$

Indeed, the inclusion $\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m)$ holds because, given $PK$ and $m$, the encrypter can compute $c$ with only field operations, and hence $c \in \mathbb{Q}(PK, m)$. The inclusion $\mathbb{Q}(PK, m) \subset \mathbb{Q}(SK, c)$ holds because, given $SK$ and $c$, the legitimate decrypter Alice can recover $m$ with only field operations.

Let's now inspect the degrees of these field extensions. Set $n = [\mathbb{Q}(SK) : \mathbb{Q}(PK)]$. Then $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)]$ is at most $n$, since adjoining $c$ to both fields can only reduce the degree of the minimal polynomial of $SK$ over $\mathbb{Q}(PK)$. We show that $\mathbb{Q}(SK, c) = \mathbb{Q}(SK, m)$. We know $\mathbb{Q}(SK, c) \supset \mathbb{Q}(SK, m)$ from the tower of fields above. Furthermore, given $SK$ anyone can recompute $PK$ since $\mathbb{Q}(PK) \subset \mathbb{Q}(SK)$, and given $PK$ and $m$ anyone can recompute $c$. Therefore, $\mathbb{Q}(SK, m) \supset \mathbb{Q}(SK, c)$. We deduce that $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)] = [\mathbb{Q}(SK, m) : \mathbb{Q}(PK, m)]$. Since $m$ is a general real number, $[\mathbb{Q}(SK, m) : \mathbb{Q}(PK, m)]$ also equals $n$. Applying the Tower Law, we have that $[\mathbb{Q}(PK, m) : \mathbb{Q}(PK, c)][\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)] = [\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)]$. Since $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)]$ is at most $n$, and since $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)]$ is exactly $n$, we see that $[\mathbb{Q}(PK, m) : \mathbb{Q}(PK, c)]$ must equal 1. Hence, $\mathbb{Q}(PK, m) = \mathbb{Q}(PK, c)$. Therefore the message $m$ lies in the adversary's field. Since the adversary has unbounded computational time, and since his field $\mathbb{Q}(PK, c)$ is countable, he can enumerate each of the elements of his field and run the public encryption algorithm on each of them until he finds the unique message $m$ which encrypts to $c$.

Hence, for the above scenario, any encryption scheme is not secure. So we modify the scenario in a couple of ways. Suppose instead of a single secret key $SK$ and a single public key $PK$, Alice uses $n$ secret keys $SK_1, ..., SK_n$, and $m$ public keys $PK_1, ..., PK_m$. If each $SK_i$ is algebraic over $\mathbb{Q}(PK_1, ..., PK_m)$, $[\mathbb{Q}(SK_1, ..., SK_n) : \mathbb{Q}(PK_1, ..., PK_m)]$ will still be finite. Replacing $SK$ with $SK_1, ..., SK_n$ and $PK$ with $PK_1, ..., PK_m$ in the above argument, we conclude that even in this case secure encryption is not possible. Note that since all parties are restricted to a finite number of operations, there can be at most a finite number of public and secret keys generated.

For now, we will continue to assume that the degree of the legitimate decrypter's field over the adversary's field is finite. For convenience, we will assume that there is one secret key $SK$ and one public key $PK$. From the results in the previous paragraph, the following arguments easily generalize to the case of multiple public-secret keys in so long as each secret key is algebraic over the field $\mathbb{Q}(PK_1, ...PK_m)$ where $m$ is the number of public keys. Whereas before we restricted the encrypter to field operations when encrypting a message $m$, we now allow the encrypter to sample real numbers as he encrypts and we allow the adversary to sample real number as well.

We first show that giving the adversary the power to sample real numbers will not help him. The encrypter will have the field $\mathbb{Q}(PK, m, r_1, ..., r_m)$ where $r_i$ is a sampled real number for all $i$. Note that the number of real numbers sampled is necessarily finite. Now, the adversary has the field $\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m, r_1, ...r_m)$. For the adversary to gain anything by sampling real numbers, he must be able to generate, via sampling and field operations, an element of $\mathbb{Q}(PK, m, r_1, r_2, ..., r_m) \setminus \mathbb{Q}(PK, c)$. Suppose he draws $m$ random reals $s_1, ..., s_m$. He now has the field $\mathbb{Q}(PK, c, s_1, ..., s_m)$. Every element of his field has the form $p(PK, c, s_1, ..., s_m)/q(PK, c, s_1, ..., s_m)$, for $p$ and $q$ polynomials with rational coefficients in the indeterminates $PK, c, s_1, ..., s_m$. To generate an element $y$ in $\mathbb{Q}(PK, m, r_1, ..., r_m) \setminus \mathbb{Q}(PK, c)$, we must have some expression $p(PK, c, s_1, ..., s_m)/q(PK, c, s_1, ..., s_m) = y$. We know that $p/q$ is not in $\mathbb{Q}(PK, c)$ since $y$ is assumed not to lie in $\mathbb{Q}(PK, c)$. Note that not all of the coefficients of the $s_i$ in the expression $p/q$ can be zero and not all of the $s_i$ in $p$ can cancel with those in $q$; for example, we cannot have the cancellation $(s_1 + s_2)/(2(s_1 + s_2)) = 1/2$, for then $p/q$ would actually be an element of $\mathbb{Q}(PK, c)$. But then we have found a nontrivial relation among the $s_i$ over the field $\mathbb{Q}(PK, c)$. If the $s_i$ are random real numbers, this occurs with probability zero since the field $\mathbb{Q}(PK, c)$ is countable, whereas the real numbers are uncountable. Hence, sampling does not help the adversary.

We now allow the encrypter to probabilistically encrypt; that is to say, we give him the ability to sample real numbers. We still necessarily have the tower of fields $\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m) \subset \mathbb{Q}(SK, c)$, where, if the encryption scheme is to be secure, then each of the above inclusions must be a proper inclusion. However, the encrypter's field is no longer $\mathbb{Q}(PK, m)$, but rather $\mathbb{Q}(PK, m, r_1, ...r_m)$, where each $r_i$ is a sampled real number. However, the argument given above still implies that the inclusions in this tower cannot be proper. That is to say, $\mathbb{Q}(PK, c) = \mathbb{Q}(PK, m)$. Hence, even if the adversary is not able to recover the original field $\mathbb{Q}(PK, m, r_1, ...r_m)$ of the encrypter, he can still recover $\mathbb{Q}(PK, m)$ and hence recover $m$.

We now consider the case where $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ is infinite. We still want the inclusions in the tower of fields

$$\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m) \subset \mathbb{Q}(SK, c),$$

to be proper.

We want both to be able to encrypt an arbitrary real number $m$ and to have a ciphertext $c$ decrypt to a unique message $m$. Hence, the number of distinct ciphertexts is at least as large as the number of distinct messages. These observations imply that the number of possible ciphertexts is uncountably infinite. Since any element $y$ which is algebraic over $\mathbb{Q}(SK)$ is in the algebraic closure of $\mathbb{Q}(SK)$, and since the algebraic closure of $\mathbb{Q}(SK)$ is countable, there is zero probability that the ciphertext $c$ will be algebraic over $\mathbb{Q}(SK)$. Hence, $c$ is transcendental over $\mathbb{Q}(SK)$ with probability 1.

Since $c$ is transcendental over $\mathbb{Q}(SK)$, and hence over $\mathbb{Q}(PK)$, the intermediate fields of $\mathbb{Q}(SK, c)/\mathbb{Q}(PK, c)$ are of the form $L(c)$, where $L$ is an intermediate field of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$. By Lüroth's theorem, all intermediate fields of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$ have the form $\mathbb{Q}(u)$, where $u$ has the form $p(SK)/q(SK)$, for $p$ and $q$ are polynomials with coefficients in $\mathbb{Q}$ in the indeterminate $SK$ and $q \neq 0$. For the inclusions in the above tower of fields to be proper, $\mathbb{Q}(PK, m)$ must be of the form $\mathbb{Q}(u, c)$. But $u$ has the form $p(SK)/q(SK)$ with $u \notin \mathbb{Q}(PK, c)$, and such a $u$ is impossible for the encrypter to generate since all he has are $PK$ and $m$, which are each algebraically independent of $SK$. Even if he were to sample real numbers, he has zero probability of generating an element $u$ of the form $p(SK)/q(SK)$. Therefore the field $\mathbb{Q}(PK, m)$ cannot contain an element of the form $p(SK)/q(SK)$, and therefore $\mathbb{Q}(PK, m)$ is forced to equal $\mathbb{Q}(PK, c)$.

## 5 The Impossibility of Secure Signature Schemes

We now shift our attention to the possibility of secure signature schemes in this model. We will show the strongest possible result, that even one-time signature schemes cannot exist.

We first need to define exactly what we mean by a signature scheme. We would like the signer to be able to sign an arbitrary real number $m$ that is not fixed at the time of key generation. If we were to remove this constraint and instead allow the signer to specify a finite sequence of messages $m_1, ..., m_N$ which he would like to be able to sign with a given keypair, secure signature schemes would in fact be possible. A secure signature scheme can be built on the fact that finding a square root of an arbitary real number $r$ is impossible in the field $\mathbb{Q}(r^2)$. Let Alice be the signer, Bob the verifier. Here's the protocol:

1. Initialization: Alice decides upon a finite sequence of messages $(m_1, m_2, ..., m_N)$ she would like to be able to sign with the public-secret keypair she is about to create. She then samples $N$ real numbers $r_1, r_2, ..., r_N$. The ordered set $(r_1, r_2, ..., r_N)$ forms Alice's secret key. Alice publishes the two ordered sets $(r_1^2, r_2^2, ..., r_N^2)$ and $(m_1, m_2, ..., m_N)$.
2. Signing: To sign the message $m_i$ for $1 \leq i \leq N$), Alice sends the pair $(m_i, r_i)$.
3. Verifying: Bob verifies the pair $(m_i, s)$ by computing $i$ from $m_i$ and checking that $s^2 = r_i^2$.

It is easy to verify the security of the above signature scheme. Also, since all parties are given unbounded computational time, $N$ can be chosen to be arbitrarily large.

We can improve this signature scheme by reducing the number of real numbers sampled to exactly one. This more efficient protocol is based on the fact that finding an $n$th root of an arbitrary real number $r$ is impossible in the field $\mathbb{Q}(r)$. Here's the protocol:

1. Initialization: Alice decides upon a finite ordered set of messages $(m_1, m_2, ..., m_N)$ she would like to sign with the key pair she is about to generate. She

then calls the subroutine $primeConvolve(N)$, described below to get the ordered set $(n_1, n_2, ..., n_N)$ and the integer $P$. She samples a real number $r$, which is her secret key. She publishes the ordered sets $(m_1, m_2, ..., m_N)$ and $(n_1, n_2, ..., n_N)$ along with the real number $r^P$ and the integer $P$.

2. Signing: To sign the message $m_i$ for $1 \leq i \leq N$, Alice sends the pair $(m_i, u^{n_i})$.
3. Verifying: Bob verifies the pair $(m_i, s)$ by computing $i$ from $m_i$ and checking that $s^{(P/n_i)} = r^P$.

We describe the subroutine $primeConvolve(N)$ in English. For every nonempty subset $S$ of $\{1, 2, ..., N\}$, the subroutine chooses a unique prime $p_S$. It then defines $t_i$ for $1 \leq i \leq N$ to be the product $\Pi_{i \in S} p_S$. Finally, it returns the ordered set $(t_1, ..., t_n)$ and the product $\Pi_{S \subset \{1,...,N\}} p_S$.

$PrimeConvolve(N)$ is used to thwart a gcd attack by an adversary who uses an adaptive chosen-message attack. $PrimeConvolve(N)$ generates a set $T$ of $N$ elements with the property that $\forall T' \subset T$, the $\gcd(y \in T')$ does not divide $x$ for $x \in T \setminus T'$. For example, calling $primeConvolve(3)$ could return the set

$$(2 \cdot 7 \cdot 11 \cdot 17, 3 \cdot 7 \cdot 13 \cdot 17, 5 \cdot 11 \cdot 13 \cdot 17)$$

and the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$. If, for example, messages $m_1$ and $m_2$ have been signed, then an adversary will learn $r^{(2 \cdot 7 \cdot 11 \cdot 17)}$ and $r^{(3 \cdot 7 \cdot 13 \cdot 17)}$, from which he can compute $gcd(r^{(2 \cdot 7 \cdot 11 \cdot 17)}, r^{(3 \cdot 7 \cdot 13 \cdot 17)}) = r^{(7 \cdot 17)}$. This is the smallest power of $r$ that can be obtained by the adversary if $r$ was chosen to be a random real number. Now, 7 does not divide $5 \cdot 11 \cdot 13 \cdot 17$; so an adversary cannot compute $r^{(5 \cdot 11 \cdot 13 \cdot 17)}$ so it is not possible for him to forge message $m_3$.

The above two signature schemes suffer because the message space is fixed to a finite subset of the real numbers at the time of key generation. We now show that, if we remove this constraint and instead allow Alice the ability to sign arbitrary real numbers after the time of key generation, then even one-time schemes are not secure.

Suppose Alice starts with the field $\mathbb{Q}$. She then samples a random real number $SK$ that will be her secret key. She is left with the field $\mathbb{Q}(SK)$. Suppose she then performs some finite number of field operations in the field $\mathbb{Q}(SK)$ to compute her public key $PK$, another element of $\mathbb{Q}(SK)$. She then publishes $PK$. We consider the case where the degree $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ is finite. Let $m$ be the message to be signed, $\sigma(m)$ its signature. For the moment, suppose that $\sigma(m)$ can be generated from $\mathbb{Q}(SK, m)$ with field operations alone. We would like the inclusions in the following tower of fields to be proper:

$$\mathbb{Q}(PK, m) \subset \mathbb{Q}(PK, m, \sigma(m)) \subset \mathbb{Q}(SK, m)$$

The leftmost field is known by an adversary trying to forge the signature $\sigma(m)$. The rightmost field is known by the legitimate signer Alice. The field in between is known by all after $m$ has been signed. If the inclusion $\mathbb{Q}(PK, m) \subset \mathbb{Q}(PK, m, \sigma(m))$ were not proper, the adversary could run the public verification algorithm on each element of his field to determine if it is in fact a valid signature for $m$. Since his field is enumerable, he will find $\sigma(m)$ in finite time.

We also want the inclusion $\mathbb{Q}(PK, m, \sigma(m)) \subset \mathbb{Q}(SK, m)$ to be proper. Otherwise, after viewing one signature $\sigma(m)$, anyone could enumerate through the field $\mathbb{Q}(PK, m, \sigma(m))$ to discover Alice's secret key $SK$.

Since $m$ is a general real, $m$ is transcendental over $\mathbb{Q}(SK)$, and hence over $\mathbb{Q}(PK)$. Therefore, the intermediate fields of $\mathbb{Q}(SK, m)/\mathbb{Q}(PK, m)$ all have the form $L(m)$, where $L$ is an intermediate field of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$. Now, in the case $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ finite, there are only a finite number of intermediate fields of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$. After one message $m$ has been signed, the public learns the field $\mathbb{Q}(PK, m, \sigma(m)) = L(m)$ for some $L$. Hence, given any future message $m'$ to be signed, the probability that the signature $\sigma(m')$ is in the field $L(m')$ is nonzero. Since an adversary has learned the field $L$, he can simply adjoin the message $m'$ to the field $L$, obtaining the field $L(m')$. He can then enumerate elements of this field until he finds $\sigma(m')$, which can be verified using the public verification algorithm. The probability that he forges an arbitrary future message $m'$ is nonzero. Therefore, after obtaining the signature for only one message, there is a nonnegligible probability that the signature of any future message can be forged. Hence, even one-time signature schemes are not possible in this model.

We now allow parties to sample real numbers. Intuitively, sampling real numbers cannot help the adversary since only a countable subset of the real numbers helps, and he is drawing from an uncountable set; see Section 3.2 for more detail. Now, if the signer is allowed to sample real numbers, the tower of fields changes to

$$\mathbb{Q}(PK, m) \subset \mathbb{Q}(PK, m, \sigma(m)) \subset \mathbb{Q}(SK, m, r).$$

For the signature scheme to be secure, each of the above inclusions must be a proper inclusion. We may not have the inclusion $\mathbb{Q}(PK, m, \sigma(m)) \subset \mathbb{Q}(SK, m)$, so the argument given above does not apply. Note, however, if there exists a message $m$ whose signature $\sigma(m)$ does not lie in the field $\mathbb{Q}(SK, m)$, then it is necessarily transcendental over $\mathbb{Q}(PK, m)$. This assertion follows from Lüroth's theorem; see Section 2. But then there can be no public verification algorithm involving $PK, m$, and $\sigma(m)$ over $\mathbb{Q}$ since $\sigma(m)$ does not satisfy any algebraic relation over $\mathbb{Q}(PK, m)$.

Finally, we consider the case where $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ is infinite. The analysis in this case is similar to that given in the previous case where we allowed the signer to use randomness. As always, we want the inclusions in the following tower of fields to be proper:

$$\mathbb{Q}(PK, m) \subset \mathbb{Q}(PK, m, \sigma(m)) \subset \mathbb{Q}(SK, m)$$

Since $SK$ is transcendental over $\mathbb{Q}(SK)$, Lüroth's theorem tells us that the only intermediate fields of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$ are transcendental extensions of $\mathbb{Q}(PK)$. Therefore, all intermediate fields of $\mathbb{Q}(SK, m)/\mathbb{Q}(PK, m)$ are transcendental extensions of $\mathbb{Q}(PK, m)$. If the signature scheme is to be secure, $\sigma(m)$ cannot be in $\mathbb{Q}(PK, m)$. Then $\mathbb{Q}(PK, m, \sigma(m))$ would necessarily be a transcendental extension of $\mathbb{Q}(PK, m)$, and hence, $\sigma(m)$ would be transcendental over

$\mathbb{Q}(PK, m)$. As we argued previously, in this case, there can be no public verification algorithm of $\sigma(m)$ over $\mathbb{Q}(PK, m)$ because $\sigma(m)$ does not satisfy any algebraic relation over $\mathbb{Q}(PK, m)$.

## 6 The Impossibility of Secret Sharing

We now generalize the impossibility of public-key encryption in this model to the impossibility of sharing a secret. The impossibility of sharing a secret will immediately rule out public-key encryption, interactive encryption, Diffie-Hellman key exchange, and oblivious transfer. We will consider an arbitrary two-party protocol and show that no such protocol establishes a shared secret.

A protocol between Alice and Bob consists of a sequence of steps. Let $F_A$ be the field generated by Alice and let $F_B$ be the field generated by Bob. During each step information may be revealed to the public. Let $F_P$ be the field generated by the public information. There are two types of steps, either Alice (Bob) selects a random element thereby extending her associated field or Alice (Bob) transmits an element from her field to Bob (Alice). Due to the transmission a transmitted element is revealed to the public.

**Step 1.** *A trancedental element $x$ over $\mathbb{Q}(F_A, F_B)$ is selected by Alice:*

$$(F_A, F_B, F_P) \rightarrow (F_A(x), F_B, F_P),$$

*or a trancedental element $x$ over $\mathbb{Q}(F_A, F_B)$ is selected by Bob:*

$$(F_A, F_B, F_P) \rightarrow (F_A, F_B(x), F_P).$$

**Step 2.** *Alice selects an element $x$ in $F_A$ and transmits it to Bob:*

$$(F_A, F_B, F_P) \rightarrow (F_A, F_B(x), F_P(x)),$$

*or Bob selects an element $x$ in $F_B$ and transmits it to Alice:*

$$(F_A, F_B, F_P) \rightarrow (F_A(x), F_B, F_P(x)).$$

To show the impossibility of secret sharing over rational numbers we need to prove

$$F_A \cap F_B = F_P \tag{1}$$

after each step of the protocol. In other words all shared information can be computed by the public by means of field operations. In the unbounded computing model there does not exist a secret since the field $F_P$ is countable. We need to prove that (1) is invariant under steps 1 and 2.

In the remainder we assume w.l.o.g. that Bob selects $x$ in both steps. Steps 1 and 2 are invariant under:

**Invariant 1.** *$F_A$, $F_B$, and $F_P$ are fields such that $F_P \subseteq F_A \cap F_B$. Furthermore $F_A = \mathbb{Q}(A)$ and $F_B = \mathbb{Q}(B)$ for finite sets of real numbers $A$ and $B$.*

*Proof.* From the invariant we infer that $F_P \subseteq F_A \cap F_B \subseteq F_A \cap F_B(x)$ and secondly $F_P(x) \subseteq (F_A \cap F_B)(x) \subseteq F_A(x) \cap F_B(x) = F_A(x) \cap F_B$ for $x \in F_B$. $\square$

In general however, we can not prove that $F_A \cap F_B = F_P$ is invariant under step 2. For example, take $F_A = \mathbb{Q}(\sqrt{6}, \sqrt{15})$, $F_B = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, $F_P = \mathbb{Q}$, and $x = \sqrt{2} \in F_B$. Clearly, $F_A(x) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ implying that $F_A(x) \cap F_B = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ while $F_P(x) = \mathbb{Q}(\sqrt{2})$.

Thus in order to prove that (1) is invariant under steps 1 and 2 we need to introduce a stronger invariant.

**Lemma 1.** *Let $G \subseteq F$ be fields such that $[G(v) : G] = [F(v) : F]$. Then either $v$ is trancedental over $F$ or there exists a basis $\mathcal{X} = \{1, v, v^2, \ldots, v^{n-1}\}$ of $F(v)$ over $F$ which is also a basis of $G(v)$ over $G$.*

*Proof.* The basis $\mathcal{X}$ of $F(v)$ over $F$ is linear independent over $G \subseteq F$. Since $[G(v) : G] = [F(v) : F]$ and $\mathcal{X}$ does not depend on $F$, $\mathcal{X}$ is a basis of $G(v)$ over $G$. $\square$

Now we are ready to formulate the stronger invariant.

**Invariant 2.** *There exist real numbers $a_i$, $1 \leq i \leq n$, such that*

$$F_B = F_P(a_1, a_2, \ldots, a_n)$$

*and*

$$\mathbb{Q}(F_A, F_B) = F_A(a_1, a_2, \ldots, a_n)$$

*with*

$$[F_A(a_1, \ldots, a_{i+1}) : F_A(a_1, \ldots, a_i)] = [F_P(a_1, \ldots, a_{i+1}) : F_P(a_1, \ldots, a_i)]$$

*for all $0 \leq i \leq n-1$.*

Initially, $F_A = F_B = F_P = \mathbb{Q}$ and invariant 2 holds for $n = 0$. The next lemmas will be used to prove that invariant 2 implies (1).

**Lemma 2.** *Let $G \subseteq F$ and let $v$ be trancedental over $F$. Then $F \cap G(v) = G$.*

*Proof.* Let $x \in G(v)$. Then there exist polynomials $f(.)$ and $g(.)$ with coefficients in $G \subseteq F$ and $g(v) \neq 0$ such that $x = f(v)/g(v)$. If $x$ is also in $F$ then either $v$ is algebraic over $F$ or $f(v)/g(v)$ does not depend on $v$, that is $x \in G$. $\square$

We define the vector space

$$G[\mathcal{X}] = \left\{ x = \sum_{\gamma \in \mathcal{X}} x_\gamma \cdot \gamma : x_\gamma \in G \right\}.$$

If $\mathcal{X}$ is a basis of $G(v)$ over $G$ then $G(v) = G[\mathcal{X}]$.

**Lemma 3.** *Let $G \subseteq F$ and let $\mathcal{X}$ be a finite linear independent set over $F$ with $1 \in \mathcal{X}$. Then $F \cap G[\mathcal{X}] = G$.*

*Proof.* Let $x \in G[\mathcal{X}]$. Then there exist coefficients $x_\gamma \in G \subseteq F$ such that $x = \sum_{\gamma \in \mathcal{X}} x_\gamma \cdot \gamma$. If $x$ is also in $F$ then $x = x_1 \in G$ since $\mathcal{X}$ is linearly independent over $F$. □

**Theorem 1.** *Invariant 2 implies $F_A \cap F_B = F_P$.*

*Proof.* Let $F_i = F_A(a_1, \ldots, a_i)$ and $G_i = F_P(a_1, \ldots, a_i)$. By lemma 1, invariant 2 implies either $a_{i+1}$ is trancedental over $F_i$ or there exists a basis $\mathcal{X}$ of $F_i(a_{i+1})$ over $F_i$ which is also a basis of $G_i(a_{i+1})$ over $G_i$. According to lemmas 2 and 3 respectively, $F_i \cap G_i(a_{i+1}) = G_i$. Since $F_A \subseteq F_i$, $F_A \cap G_i(a_{i+1}) \subseteq G_i$, that is

$$F_A \cap G_{i+1} = F_A \cap G_i(a_{i+1}) \subseteq F_A \cap G_i.$$

Hence,

$$F_P \subseteq F_A \cap F_B = F_A \cap G_n \subseteq \ldots \subseteq F_A \cap G_0 = F_A \cap F_P = F_P.$$

□

The next invariant is like invariant 2 where the $A$'s and $a$'s are interchanged with the $B$'s and $b$'s. Because of the symmetry theorem 1 also holds for this invariant.

**Invariant 3.** *There exist real numbers $b_i$, $1 \leq i \leq m$, such that*

$$F_A = F_P(b_1, b_2, \ldots, b_n)$$

*and*

$$\mathbb{Q}(F_A, F_B) = F_B(b_1, b_2, \ldots, b_m)$$

*with*

$$[F_B(b_1, \ldots, b_{i+1}) : F_B(b_1, \ldots, b_i)] = [F_P(b_1, \ldots, b_{i+1}) : F_P(b_1, \ldots, b_i)]$$

*for all $0 \leq i \leq m - 1$.*

The next lemmas are used to show that invariants 2 and 3 are equivalent. The proof of Lemma 5 is left to the appendix.

**Lemma 4.** *Consider the chain of fields $G \subseteq H \subseteq F$ and suppose that $[F(v) : F] = [G(v) : G]$. Then $[F(v) : F] = [H(v) : H] = [G(v) : G]$.*

*Proof.* According to lemma 1 either $v$ is trancedental over $F$ or there exists a basis $\mathcal{X}$ of $F(v)$ over $F$ which is also a basis of $G(v)$ over $G$. If $v$ is trancedental over $F$ then it is also trancedental over its subfields $G$ and $H$ in which case $[F(v) : F] = [H(v) : H] = [G[v] : G] = \infty$. If $\mathcal{X}$ is a basis over $F$ then it is linear independent over $H$, hence $[H(v) : H] \geq [F(v) : F]$. If $\mathcal{Y}$ is a basis over $H$ then it is linear independent over $G$, hence $[G(v) : G] \geq [H(v) : H]$. Since $[F(v) : F] = [G(v) : G]$, equalities hold everywhere. □

**Lemma 5.** *Let $G$ be a field. If $[G(u,v):G(u)] = [G(v):G]$ then also $[G(v,u):G(v)] = [G(u):G]$.*

**Theorem 2.** *Invariants 2 and 3 are equivalent.*

*Proof.* Suppose that invariant 2 holds. By invariant 1 there exist real numbers $b_i$, $1 \le i \le m$, such that $F_A = F_P(b_1, b_2, \ldots, b_m)$. Let

$$H_{i,j} = F_P(a_1, \ldots, a_i)(b_1, \ldots, b_j),$$

$F_i = F_A(a_1, \ldots, a_i)$, and $G_i = F_P(a_1, \ldots, a_i)$. Notice that $H_{n,j} = F_B(b_1, \ldots, b_j)$, $H_{0,j} = F_P(b_1, \ldots, b_j)$, and $H_{n,m} = \mathbb{Q}(F_A, F_B)$. Clearly, $G_i \subseteq H_{i,j} \subseteq H_{i,j}(b_{j+1}) \subseteq F_i)$. By using invariant 2 and twice applying lemma 4 we obtain

$$\begin{aligned}[F_i(a_{i+1}):F_i] &= [H_{i,j}(b_{j+1}, a_{i+1}) : H_{i,j}(b_{j+1})] \\ &= [H_{i,j}(a_{i+1}) : H_{i,j}] = [G_i(a_{i+1}) : G_i].\end{aligned}$$

By lemma 5 we conclude $[H_{i,j}(b_{j+1}, a_{i+1}) : H_{i,j}(a_{i+1})] = [H_{i,j}(b_{j+1}) : H_{i,j}]$, that is

$$[H_{i+1,j+1} : H_{i+1,j}] = [H_{i,j+1} : H_{i,j}].$$

Repeating this process gives

$$[H_{n,j+1} : H_{n,j}] = [H_{0,j+1} : H_{0,j}],$$

which is equivalent to invariant 3. $\square$

Notice that the above proof holds for all real numbers $b_i$, $1 \le i \le m$, such that $F_A = F_P(b_1, b_2, \ldots, b_m)$. We may reformulate both invariants accordingly.

Now we are ready to prove the correctness of both invariants under steps 1 and 2. Consider step 1. Bob selects a trancedental element $x$ over $\mathbb{Q}(F_A, F_B)$. Take $a_{n+1} = x$. Notice that

$$[\mathbb{Q}(F_A, F_B)(x) : \mathbb{Q}(F_A, F_B)] = [\mathbb{Q}(F_B)(x) : \mathbb{Q}(F_B)]. \tag{2}$$

Hence, invariant 2 holds again:

$$F_B(x) = F_P(a_1, \ldots, a_{n+1})$$

and

$$\mathbb{Q}(F_A, F_B(x)) = \mathbb{Q}(F_A, F_B)(x) = F_A(a_1, \ldots, a_{n+1})$$

together with the corresponding degree requirements.

Consider step 2. Bob selects an element $x \in F_B$ which he transmits to Alice. Invariant 3 holds prior to this step: $F_A = F_P(b_1, \ldots, b_m)$ and $\mathbb{Q}(F_A, F_B) = F_B(b_1, \ldots, b_m)$ with

$$[F_B(b_1, \ldots, b_{i+1}) : F_B(b_1, \ldots, b_i)] = [F_P(b_1, \ldots, b_{i+1}) : F_P(b_1, \ldots, b_i)]$$

for $0 \leq i \leq m-1$. Notice that $F_P \subseteq F_P(x) \subseteq F_B$. By repeadetly applying lemma 4 we obtain

$$[F_B(b_1, \ldots, b_{i+1}) : F_B(b_1, \ldots, b_i)] = [F_P(x)(b_1, \ldots, b_{i+1}) : F_P(x)(b_1, \ldots, b_i)]$$

for $0 \leq i \leq m-1$. Since $F_A(x) = F_P(x)(b_1, \ldots, b_m)$ and $\mathbb{Q}(F_A(x), F_B) = \mathbb{Q}(F_A, F_B) = F_B(b_1, \ldots, b_m)$, invariant 3 holds again. By theorem 2 both invariants hold again after each step.

**Theorem 3.** *Invariants 2 and 3 are invariant under steps 1 and 2.*

The proof of the invariants being invariant under step 1 only requires the condition (2), which is satisfied for step 1 because $x$ is trancedental over $\mathbb{Q}(F_A, F_B)$.

## 7 Conclusion

In summary, we have shown that although authentication protocols and one-way functions exist in the this model, secure signature schemes, secure encryption schemes, and secret sharing schemes do not. If we replace the operations {+, -, *, /} with the operations {+, -, *, /, $x^y$}, where $x^y$ denotes the operation of raising an arbitrary number $x$ to an arbitrary power $y$, we are able to recover many cryptographic primitives, such as Diffie-Hellman Key Exchange, secure signature schemes, and secure encryption schemes. Of course we still allow all parties the ability to sample real numbers. We would like to determine a set of necessary and sufficient conditions for a set of operations to admit certain cryptographic primitives.

## 8 Acknowledgments

Special thanks to Ron Rivest for helping frame these problems as field-theoretic problems. Also, thanks to Xiaowen Xin for helping prepare this document and for motivation.

## References

1. Artin, M., "Algebra," Prentice-Hall, 1991.
2. Burmester, M., Rivest, R., Shamir, A., *Geometric Cryptography*, http://theory.lcs.mit.edu/˜rivest/publications.html, 1997.
3. Kaplansky, I., "Fields and Rings," Second Edition, University of Chicago Press, 1972.
4. Morandi, P., "Field and Galois Theory, Graduate Texts in Mathematics," Volume 167, Springer-Verlag, 1996.
5. Rompel, J., *One-way Functions are Necessary and Sufficient for Secure Signatures*, ACM Symp. on Theory of Computing **22** (1990), 387-394.

# A Proof of Lemma 5

If $[G(u,v):G(u)] = [G(v):G] < \infty$ then the proof follows from

$$[G(u,v):G(u)][G(u):G] = [G(u,v):G] = [G(v,u):G(v)][G(v):G].$$

If $[G(u,v):G(u)] = [G(v):G] = \infty$ then $v$ is trancedental over $G(u)$. We distinguish two cases. Firstly, if $u$ is trancedental over $G(v)$ then it is also trancedental over $G$, hence, $[G(v,u):G(v)] = [G(u):G] = \infty$.

Secondly, suppose that $u$ is algebraic over $G(v)$. We will show that $u$ is algebraic over $G$ and that a basis of $G(u)$ over $G$ is also linearly independent over $G(v)$, which implies $[G(u):G] \leq [G(v,u):G(v)]$. A basis $\mathcal{X} = \{1, u, u^2, \ldots, u^{n-1}\}$ of $G(v,u)$ over $G(v)$ exists and is also linearly independent over $G$ and part of $G(u)$, which implies $[G(u):G] \geq [G(v,u):G(v)]$ and equality must hold.

We are in the case that $v$ is trancedental over $G(u)$ and $u$ is algebraic over $G(v)$. Then there exist a finite and strictly positive number of non-zero coefficients $u_i \in G(v)$ such that $0 = \sum_i u_i \cdot u^i$. Each coefficient $u_i$ is in $G(v)$ and can be expressed as $u_i = f_i(v)/g_i(v)$, where $f_i(.)$ and $g_i(.)$ are polynomials with coefficients in $G$. Define $h_i(v) = f_i(v)\prod_{j\neq i} g_j(v)$. Then $\sum_i h_i(v)\cdot u^i = 0$. Polynomial $h_i(.)$ has coefficients in $G$, therefore $h_i(v) = \sum_j h_{i,j}\cdot v^j$ for finitely many non-zero coefficients $h_{i,j} \in G$. We obtain

$$0 = \sum_j \left\{ \sum_i h_{i,j}\cdot u^i \right\} \cdot v^j.$$

The inner sums are in $G(u)$. Since $v$ is trancedental over $G(u)$, these inner sums are equal to 0. If $u$ is trancedental over $G$ then all coefficients $h_{i,j} = 0$. This implies that $h_i(v) = 0$. All $f_j(v) \neq 0$, therefore $g_i(v) = 0$, hence, $u_j = 0$. However, there is a strictly positive number of non-zero coefficients $u_j$. Concluding, $u$ is not trancedental but algebraic over $G$.

Since $u$ is algebraic over $G$ there exists a finite basis $\mathcal{X}$ of $G(u)$ over $G$ with $G(u) = G[\mathcal{X}]$. We want to show that $\mathcal{X}$ is linearly independent over $G(v)$. Suppose that $\sum_{\gamma\in\mathcal{X}} x_\gamma \cdot \gamma = 0$ for some $x_\gamma \in G(v)$. For the coefficients $x_\gamma$ there exist polynomials $f_\gamma(.)$ and $g_\gamma(.)$ with coefficients in $G$ with $g_\gamma(v) \neq 0$ such that $x_\gamma = f_\gamma(v)/g_\gamma(v)$. Define $h_\gamma(v) = f_\gamma(v)\prod_{\sigma\neq\gamma} g_\sigma(v)$. Then $\sum_{\gamma\in\mathcal{X}} h_\gamma(v)\cdot\gamma = 0$. Polynomial $h_\gamma(.)$ has coefficients in $G$, therefore $h_\gamma(v) = \sum_j h_{\gamma,j}\cdot v^i$ for finitely many non-zero coefficients $h_{\gamma,j} \in G$. We obtain

$$0 = \sum_j \left\{ \sum_{\gamma\in\mathcal{X}} h_{\gamma,j}\cdot \gamma \right\} \cdot v^j.$$

The inner sums are in $G[\mathcal{X}] = G(u)$. Since $v$ is trancedental over $G(u)$, these inner sums are equal to 0. Set $\mathcal{X}$ is linearly independent over $G$, hence, all coefficients $h_{\gamma,j} = 0$. This implies that $h_\gamma(v) = 0$. All $f_\sigma(v) \neq 0$, therefore $g_\gamma(v) = 0$, hence, $x_\gamma = 0$.