Cryptography in an Unbounded Computational Model

by

David Paul Woodruff

Submitted to the Department of Electrical Engineering and Computer Science
in Partial Fulfillment of the Requirements for the degrees of

Bachelor of Science in Computer Science and Engineering

and

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2002

Author ....
Department of Electrical Engineering and Computer Science
May 14, 2002

Certified by ....
Ronald L. Rivest
Viterbi Professor of Computer Science and Engineering
Thesis Supervisor

Accepted by ....
Arthur C. Smith
Chairman, Department Committee on Graduate Theses

Cryptography in an Unbounded Computational Model

by

David Paul Woodruff[1]

Submitted to the
Department of Electrical Engineering and Computer Science

May 14, 2002

In Partial Fulfillment of the Requirements for the
degrees of Bachelor of Science in Computer Science and Engineering
and
Master of Engineering in Electrical Engineering and Computer Science

Abstract

In this thesis, 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.

Thesis Supervisor: Ronald L. Rivest
Title: Viterbi Professor of Computer Science and Engineering

[1]Supported by NTT grant.

Acknowledgments

I would first like to thank Professor Ronald Rivest for offering his valuable time and support as my research advisor. He first introduced this line of research to me and has helped keep my interest in it all the while. Much of my interest in cryptography in general stems from positive experiences with him.

I am also indebted to Marten van Dijk who helped me with some of the more technical aspects of this research. He has inspired me to look for other applications of algebraic number theory to cryptography.

Finally I would like to thank my parents, David and Marsha, for unconditional support and guidance.

Contents

Chapter 1

Introduction

In the classical model of computation, parties represent data with bits and have a small set of bit operations to work with. Usually some parties are restricted to a polynomial number of operations in some security parameter. Cryptographic primitives, such as signature schemes and encryptions schemes, are then constructed on top of this computational model. But cryptography may be compatible with other models as well. In this thesis we analyze the possibility of many different primitives over a novel computational model. To motivate the study of cryptography over our model, we show the existence of zero-knowledge identification protocols and authentication protocols. However, despite this positive result, we then prove the impossibility of secure signature schemes, secure public-key encryption schemes, and more generally, secure secret-key exchange.

1.1 Motivation

The computational model we consider bares little resemblance to practical, real-life models of computation. In particular, we give all parties unbounded computational time and the ability to store irrational numbers in single, infinite-precision registers. Despite this, we hope that by studying cryptography in this new model we will gain insight for the classical model. We present a new algebraic framework for studying classical cryptographic problems. For example, we frame the security of certain protocols as specific field-theoretic properties. Perhaps this formulation can be adopted in the classical setting.

1.2 Unbounded Computational Model

In our model all parties start with the two numbers zero and one. They are given the standard set of field operations $\{+, -, *, /\}$ to work with. Furthermore, they are given unbounded computational time. That is to say, parties can perform any finite number of operations but they must eventually halt. From these rules, we see that parties can generate any rational number, i.e., any number in the field $\mathbb{Q}$ of rational numbers. We define a party's *state of knowledge* as the field he can generate. We see that the state of knowledge is the same for all parties and is exactly $\mathbb{Q}$.

If this were all there were to our model, there would be no "secrets". Any party can generate the same set of numbers as any other party. More formally, suppose a party wishes to keep secret an element s of an enumerable field F. Suppose the adversary has a set of generators for F. Finally, suppose that there exists a public verification algorithm for s, i.e., a publicly computable function $p : F \to \{0, 1\}$ such that $p(x) = 1$ if and only if $x = s$. Then an adversary can determine s as follows. He simply enumerates elements f of F and computes $p(f)$ for each one until $p(f)$ evaluates to 1. When this happens, f necessarily equals s and the adversary has found the secret. Note that the adversary can enumerate F since F is enumerable and the adversary has its generators. We will refer to this type of attack as an *enumeration attack*.

In our model we mentioned the fact that all parties are restricted to the rational numbers and furthermore, can generate any rational number. Hence, the fact that $\mathbb{Q}$ is countable implies that there are no secrets. We prevent enumeration attacks with some extensions to the model. We give all parties the ability to sample any finite number of real numbers from a uniform distribution of real numbers. For technical reasons[1] we restrict sampling to the closed interval $[0, 1]$ of real numbers. To support

[1] There does not exist a uniform distribution over the entire field of real numbers.

this, we equip all parties with registers which can store arbitrary real numbers to infinite precision.

Now we see that enumeration attacks fail. Instead of just the rational numbers, parties now generate fields of the form $\mathbb{Q}(\vec{r})$ for $\vec{r} = (r_1, \dots, r_n)$ a vector of real numbers sampled at random. Even though fields of the form $\mathbb{Q}(\vec{r})$ are enumerable, parties can now keep secrets since an adversary does not have the generators $\vec{r}$. Even if the adversary samples real numbers, he has zero probability of sampling anything meaningful. Indeed, if he samples real numbers $\vec{t} = (t_1, \dots, t_n)$, there is zero chance that $\mathbb{Q}(\vec{t}) \cap \mathbb{Q}(\vec{r}) \neq \mathbb{Q}$. Formally, $\mathbf{Pr}_{\vec{t} \in [0,1]^n}[\mathbb{Q}(\vec{t}) \cap \mathbb{Q}(\vec{r}) = \mathbb{Q}] = 1$. We do not make additional modifications to the model.

1.3 One-way Functions

One of the most basic cryptographic primitives is the *one-way function*. Intuitively, this is a function which is easy to compute, but hard to invert. It is believed that one-way functions exist in the classical model of computation, but this has not been proven. In our model we do not need to speculate. 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 only r^2 and the rational field operations. Even if one were to sample real numbers, there are only a countable number of real numbers that would help, but we're sampling from an uncountable set. Formally,

$$\mathbf{Pr}_{\vec{t} \in [0,1]^n}[\mathbb{Q}(\vec{t}, r^2) \cap \mathbb{Q}(r) = \mathbb{Q}] = 1.$$

Since there is zero probability of deducing r from $\mathbb{Q}(r^2)$, the function $f(r) \rightarrow r^2$ is a one-way function in this model.

The existence of many cryptographic primitives, such as signature schemes, encryption schemes, and identification protocols, depends on the existence of one-way functions. Rompel shows that one-way functions are necessary and sufficient for secure signature schemes to exist in the standard computational model[6]. The proof relies on the bit-representation of numbers in the number field the parties work 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 arbitrary real numbers in constant time. Thus we can not assume that secure-signature schemes exist in our model because we cannot use the reductions from classical cryptography, which depend heavily on the underlying model of computation.

So we ask which cryptographic primitives exist in our model. In a similar model of computation [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 in that model? What about our model? Although the first of these questions remains unanswered, we shall see that in our model identification protocols exist but secure signatures schemes, secure public-key encryption schemes, and more generally, secure secret-key exchange protocols do not. We conjecture the same to be true of the ruler-compass constructible points.

Part of this thesis is adapted from a conference paper [7] written by Marten van Dijk and myself. The work in sections 2-5 is my individual work and the work in section 6 and the appendix is joint work with Marten van Dijk. Section 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 exchange a secret-key in this model.

Chapter 2

Algebraic Preliminaries

The proof of knowledge over the ruler-compass constructible points [2] 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 which show angle trisection is impossible[1]. 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 π are transcendental over $\mathbb{Q}$ because they do not satisfy a polynomial $p(t)$ with rational coefficients [5]. 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 linear combination of the form $f_1 v_{\alpha_1} + ... + f_n v_{\alpha_n}$, 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 [4] 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 concept of 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 [5] that the cardinality of the algebraic closure of F is also countable.

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 [5].

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[5].

The final theorem that we will need, due to Lüroth [5], 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 $q \neq 0$.

Chapter 3

An Identification Protocol

We present a zero-knowledge identification protocol, similar to that for ruler-compass constructible points[2], which is an extension of the Fiat-Shamir protocol [3]. Informally, an identification protocol is a 2-party protocol by which party A can convince party B of his identity with high probability, and any party C trying to impersonate A to B can do so with only low probability. We say an identification protocol is *complete* if A succesfully convinces B of his identity with high probability, and we say that the protocol is *sound* if any other party C successfully impersonates A to B with only low probability. The fact that the protocol is zero-knowledge means that after A's interaction with B, B does not learn much information, i.e., he gains "zero-knowledge." This prevents B from impersonating A later on after his interaction with A.

Our protocol is shown in Figure 3-1. 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. Note, even if Alice cannot decide if r is rational in this computational model, she can be assured with overwhelming probability that only she knows r. 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.

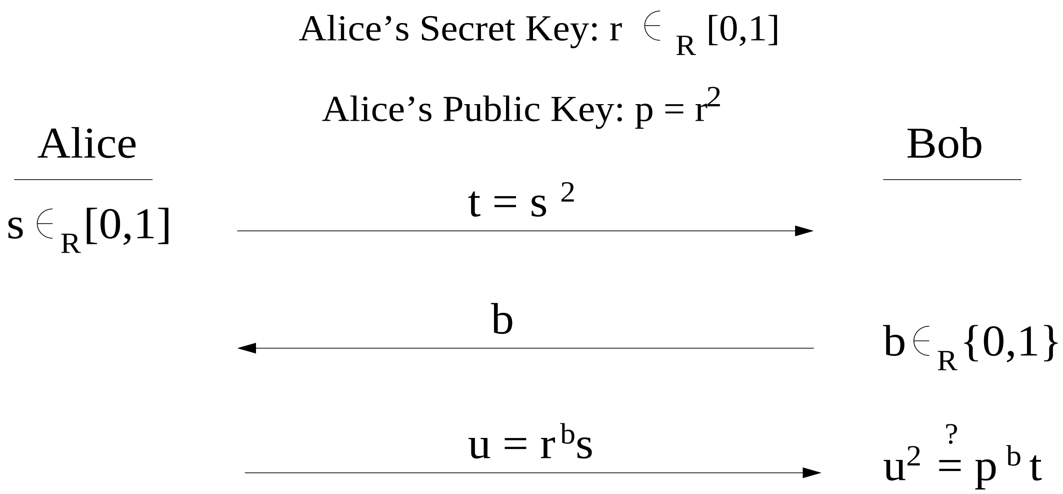

Figure 3-1: A Zero-knowledge Identification Protocol

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 a zero-knowledge identification protocol: 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, if u^2/p is less than one. Otherwise, repeat (choose u again) until u^2/p is less than one. This process is expected to terminate in a finite number of iterations. Even if

Bob is to use a nonuniform distribution, his view can be simulated by probing and resetting him[2]. 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.

This protocol can be extended to a zero-knowledge authentication protocol as was similarly done for the ruler-compass identification protocol[2].

Chapter 4

The Impossibility of Secure Public-Key Encryption

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. We will show that in any such scheme the state of knowledge (see Chapter 1) of the adversary is the same as that of the encrypter. It will follow that the adversary will be able to recover the encrypter's plaintext.

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.

Without loss of generality, we have $\mathbb{Q}(PK) \subseteq \mathbb{Q}(SK)$. This assumes that no real numbers are sampled during public-key generation. We will see later on, when we discuss schemes with multiple secret keys $SK_1, \ldots, SK_n$, that we can append whatever randomness is used in key generation to the secret key itself.

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 once the adversary has heard c. 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, we see that in the above scenario public-key encryption schemes are not secure. So we modify the scenario in a couple of ways. Suppose instead of using 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 $\mathbb{Q}(PK_1, ..., PK_m)$, $[\mathbb{Q}(SK_1, ..., SK_n) : \mathbb{Q}(PK_1, ..., PK_m)]$ is 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 messages, 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. 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 $\mathbb{Q}(PK, c)$ has measure zero in the real numbers. 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. This case could arise if, for instance, Alice samples real numbers r, s to be her secret key and sets her public key to be rs. Then clearly $\mathbb{Q}(rs) \subseteq \mathbb{Q}(r, s)$, but now $[\mathbb{Q}(r, s) : \mathbb{Q}(rs)] = \infty$. 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 to generate with only 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 $\mathbb{Q}(PK, c)$.

Chapter 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 $\mathbb{Q}(r)$. Let Alice be the signer, Bob the verifier. Here's the protocol:

1. Initialization: Alice decides upon a finite sequence of messages $(m_1, \ldots, m_N)$ she would like to be able to sign with the public-secret keypair she is about to create. She then samples N real numbers $r_1, r_2, \ldots, r_N$. The ordered set $(r_1, \ldots, r_N)$ forms Alice's secret key. Alice publishes the two ordered sets $(r_1^2, \ldots, r_N^2)$ and $(m_1, \ldots, m_N)$.

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, but finite.

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 nth 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 sequence of messages $(m_1, \ldots, m_N)$ that she would like to sign with the key pair she is about to generate. She then computes the first $N+1$ primes $(p_1, \ldots, p_{N+1})$ and she lets $P = \Pi_{i=1}^{N+1} p_i$. She samples a real number r which is her secret key. She then publishes the sequence $(m_1, \ldots, m_N)$ together with the number r^P as her public key.

2. Signing: To sign the message m_i, Alice sends the pair $(m_i, r^{P/p_i})$.

3. Verifying: Bob verifies the pair (m_i, s) by computing the first $N+1$ primes $(p_1, \ldots, p_{N+1})$ and the integer P, computing i from Alice's public key, and finally verifying that $s^{p_i} = r^P$.

This signature scheme prevents a gcd-attack as follows. If two messages m_i and m_j have been signed by Alice, the public learns $\gcd(r^{P/p_i}, r^{P/p_j}) = r^{P/(p_i \cdot p_j)}$. If someone wants to forge the signature of a new message m_k ($i \neq k$, $j \neq k$), he will have to compute r^{P/p_k} from his knowledge of $r^{P/(p_i \cdot p_j)}$. But this is not possible since $P/(p_i \cdot p_j)$ is divisible by p_k, whereas P/p_k is not. This analysis can be extended to show that if any $M \leq N$ messages have been signed, it is not possible to forge a future message. Even if all N messages have been signed, the public will only learn $r^{P/(p_1 \cdots p_N)} = r^{p_{N+1}}$, and hence cannot recover the secret key r since it is impossible to take p_{N+1}-st roots in this model.

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. Without loss of generality, we again assume that $\mathbb{Q}(PK) \subseteq \mathbb{Q}(SK)$.

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 $\mathbb{Q}(SK)/\mathbb{Q}(PK)$. See Figure 5.1. After one message m has been signed, the public learns the field $\mathbb{Q}(PK, m, \sigma(m)) = L(m)$ for some L. By enumerating elements of $L(m)$, the public also enumerates elements of L, so without loss of generality, we can say the public learns the field L.

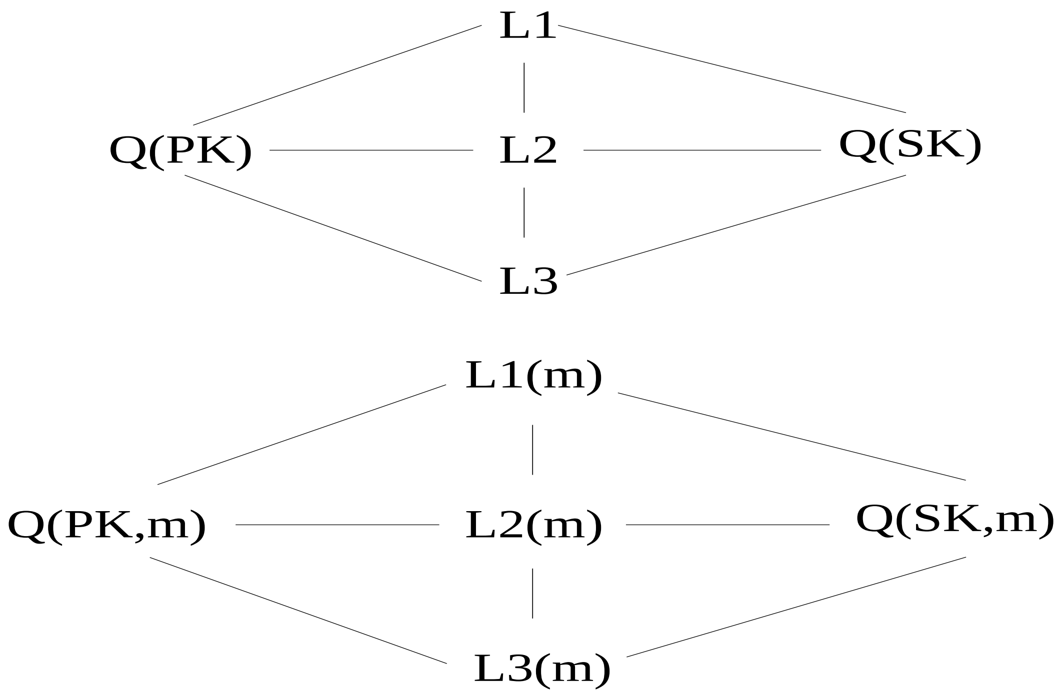

Figure 5-1: Intermediate fields of $Q(SK)/Q(PK)$ are in bijective correspondence with intermediate fields of $Q(SK,m)/Q(SK,m)$.

The adversary can now try to forge the signature of a future message. The adversary proceeds as follows. He samples an arbitrary real number m' and he forms the field $L(m')$, which he can enumerate. He enumerates elements of $L(m')$ until he finds $\sigma(m')$, which he can verify using the public verification algorithm. We now consider his chances of finding $\sigma(m')$, i.e., the probability that $\sigma(m')$ lies in $L(m')$.

In the case when $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ is finite, there are only a finite number of intermediate fields of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$. Let N be the number of such intermediate fields. As aforementioned, we are assuming the signer does not know the messages he will sign a priori, and therefore, we can think of m as a random real number which was handed to the signer by the public. Since m is a random real, and since $\sigma(m) \in L(m)$, the probability that the signature $\sigma(m')$ of a future random real m' will lie in $L(m')$ is strictly positive. For instance, if the signatures of real numbers were uniformly distributed amongst the N intermediate fields L_i of $\mathbb{Q}(SK)/\mathbb{Q}(PK)$, the probability that $\sigma(m')$ lies in any particular field $L_i(m')$ is exactly $1/N$. In the general case, since $\sigma(m) \in L(m)$, we know the probability that signatures of real numbers $\sigma(r)$ lie in $L(r)$ is nonzero.

Say that for a randomly sampled real r, the probability that $\sigma(r) \in L(r)$ is $p > 0$. Then after obtaining the signature for a random future message m', the adversary will halt having computed $\sigma(m')$ with probability p. Since this probability is nonnegligible, 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 (Chapter 2) since all intermediate fields of $\mathbb{Q}(SK, m, r)/\mathbb{Q}(SK, m)$ are of the form $\mathbb{Q}(SK, m, p(r)/q(r))$, where p and q are polynomials in r, and hence transcendental over $\mathbb{Q}(SK, m)$. 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 $\mathbb{Q}(PK, m)$.

Chapter 6

The Impossibility of Secret-Key Exchange

We now generalize the impossibility of public-key encryption in this model to the impossibility of establishing a shared secret-key. The impossibility of secret-key exchange 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-key. Note that it is possible that a three-party protocol can be used to establish a shared-secret, but we do not consider that here.

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. Due to the transmission a transmitted element is revealed to the public. Let F_P be the field generated by the public information. There are two types of steps, Alice (Bob) selects a random element thereby extending her (his) associated field or Alice (Bob) transmits an element from her (his) field to Bob (Alice).

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

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

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

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

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

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

To show the impossibility of secret-key exchange over the rational numbers we need to prove

$$F_A \cap F_B = F_P \tag{6.1}$$

holds after each step of the protocol. In other words all shared information between Alice and Bob is in fact public information. We prove that (6.1) 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 $x \in F_B$.∎

In general however, we cannot 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 (6.1) is invariant under steps 1 and 2 we introduce a stronger invariant.

Lemma 1 *Let $G \subseteq F$ be fields such that $[G(v) : G] = [F(v) : F]$. Then either v is transcendental 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 linearly 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.∎

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 $0 \leq i \leq n-1$.

See Figure 6.1. 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 (6.1).

Lemma 2 *Let $G \subseteq F$ and let v be transcendental 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 $x \in G$.∎

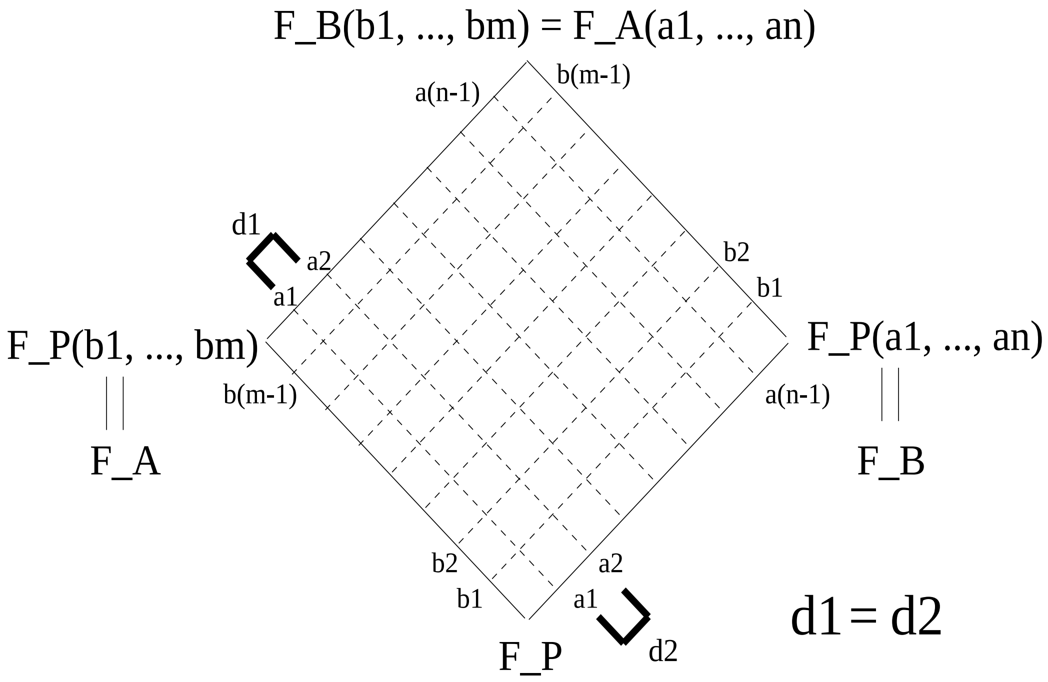

Figure 6-1: The degree between any two dashed lines is the same no matter where you are on the square. The figure shows d1 = d2.

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 linearly 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 transcendental 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,

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

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 the Parallelogram lemma is left to the appendix.

Lemma 4 *Consider the tower 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 transcendental 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 transcendental over F then it is also transcendental 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 linearly independent over H, hence $[H(v):H] \geq [F(v):F]$. If $\mathcal{Y}$ is a basis over H then it is linearly independent over G, hence $[G(v):G] \geq [H(v):H]$. Since $[F(v):F] = [G(v):G]$, equalities hold everywhere.∎

Parallelogram Lemma *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, $1 \leq i \leq m$, 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 the Parallelogram lemma 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.∎

Notice that the above proof holds for all real numbers b_i, $1 \leq i \leq m$, 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 transcendental element x over $\mathbb{Q}(F_A, F_B)$. Take $a_{n+1} = x$.

Notice that

$$[\mathbb{Q}(F_A, F_B)(x) : \mathbb{Q}(F_A, F_B)] = [\mathbb{Q}(F_B)(x) : \mathbb{Q}(F_B)]. \tag{6.2}$$

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 repeatedly 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 (6.2), which is satisfied for step 1 because x is transcendental over $\mathbb{Q}(F_A, F_B)$. This completes the proof.

Chapter 7

Conclusion

In summary, we have shown that although identification protocols and one-way functions exist in this model, secure signature schemes, secure encryption schemes, and secret-key exchange 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. This is because the discrete logarithm problem, i.e., finding x given g and g^x, remains intractable. Therefore, we can use the ElGamal signature and public-key encryption schemes without much modification in our computational model. Of course we still allow all parties the ability to sample real numbers. What is it about the operation x^y that allows much of public-key cryptography to be possible? We would like to determine a set of necessary and sufficient conditions for a set of operations to admit certain cryptographic primitives.

Appendix A

Proof of Parallelogram Lemma

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

Proof 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 transcendental over $G(u)$. We distinguish two cases. Firstly, if u is transcendental over $G(v)$ then it is also transcendental 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 $\mathcal{X} = \{1, u, u^2, \dots, u^{n-1}\}$ 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 transcendental over $G(u)$ and u is algebraic over $G(v)$. Then there exists 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 transcendental over $G(u)$, these inner sums are equal to 0. If u is transcendental 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 transcendental over G, i.e., it is algebraic.

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_γ 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 transcendental 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, $x_\gamma = 0$.

Bibliography

[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] A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” *Advances in Cryptology - Crypto ’86*, Springer-Verlag (1987), 186-194.

[4] Kaplansky, I., *Fields and Rings*, Second Edition, University of Chicago Press, 1972.

[5] Morandi, P., *Field and Galois Theory, Graduate Texts in Mathematics*, Volume 167, Springer-Verlag, 1996.

[6] Rompel, J., “One-way Functions are Necessary and Sufficient for Secure Signatures”, ACM Symp. on Theory of Computing **22** (1990), 387-394.

[7] Woodruff, D., van Dijk, M., “Cryptography in an Unbounded Computational Model”, *Proc. of Eurocrypt 2002*, Springer-Verlag (2002).