Geometric Cryptography: Identification by Angle Trisection

(Draft 2)

Mike Burmester*
Information Security Group
Royal Holloway–University of London
Egham, Surrey TW20 OEX, U.K.

Ronald L. Rivest†
Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139, U.S.A.

Adi Shamir‡
Department of Computer Science
The Weizmann Institute of Sciences
Rehovot 76100, Israel

November 4, 1997

Abstract

We propose the field of "geometric cryptography," where messages and ciphertexts may be represented by geometric quantities such as angles or intervals, and where computation is performed by ruler and compass constructions.

We describe a elegant little zero-knowledge identification scheme, based on the impossibility of trisecting an angle using ruler and compass operations.

While geometric cryptography may have little practical application, it may facilitate the construction of pedagogic examples making cryptographic principles accessible to a wider audience, and may also by contrast illuminate those cryptographic principles.

1 Geometric Cryptography

The modern theory of computation, following Turing, is based on representing data as sequences of symbols (typically bits), and performing operations from a small set of primitive operations (such as ANDs and ORs). But the notion of computation is compatible with other data representations. For example, the classic geometric notion of constructability with ruler and compass operations yields a rich theory analogous in many ways to the modern theory of computation. The impossibility of trisecting an angle can be viewed as analogous to the impossibility of solving the halting problem. The difficulty, or impossibility, of solving geometric problems can be used as a foundation for "geometric cryptography"–a field which we propose for further study. By way of getting this field of study off the ground, we propose here a simple zero-knowledge identification protocol, based on the impossibility of trisecting an angle by ruler and compass.

We begin by reviewing the standard operations allowed in ruler and compass constructions:

*email address: m.burmester@rhbnc.ac.uk
†email address: rivest@theory.lcs.mit.edu
‡email address: shamir@wisdom.weizmann.ac.il

1. Given two distinct points, one can construct the unique line on which both lie.
2. Given two distinct lines that meet, one can construct their point of intersection.
3. If A and B are distinct points, then one can construct three points C_1, C_2, and C_3, distinct from A and B, such that:
   (a) C_1 is on the line determined by A and B, and between A and B.
   (b) C_2 is on the line determined by A and B, and B is between A and C_2.
   (c) C_3 is not on the line determined by A and B.
4. If AB is any interval and CD is any ray, then one can construct a point E on CD such that AB and CE are congruent.
5. Given any circle and a line that meets it, one can construct the point(s) of intersection.

These axioms are paraphrased from the excellent survey of geometry [3]. The undefined terms (such as "points," "interval," "between," "congruent," and so on) are used in other axioms (not given here) that delimit their meaning. Given the above primitives, one can show that it is possible to perform other constructions, such as bisecting an interval or an angle, constructing a perpendicular to a line through a point on that line, or determining the point(s) of intersection of two circles. The theory of geometric constructability is a rich one. We do not elaborate this theory here, since we will be using only the simplest techniques. In "geometric cryptography," messages and ciphertexts are represented by geometric objects such as intervals or angles. More complicated representations could of course be used.

For cryptographic purposes, one needs to be able to generate and keep random "secrets" that are unpredictable to the adversary. These should not be constructable by ruler and compass from previously constructed objects, otherwise the adversary can find them. To model this within geometric cryptography, we require an additional axiom for the selection of random points.

6. One can select uniformly distributed random points in the unit circle.

Selecting such points amounts to generating secrets that are unknowable to an adversary. We also assume that parties can flip coins.

It is well known that trisecting an arbitrary angle is impossible with a ruler and (an unmarked) compass. However, tripling an angle is easy. Thus, the operation of tripling an angle is a "one-way function" for geometric cryptography.

We assume that an adversary can do unbounded computation (in the classical sense), but is limited to performing ruler and compass constructions in terms of manipulating geometric information, and to selecting random points in the plane.

2 An Identification Protocol

Alice (the Prover) wishes to establish a means of proving her identity later to Bob (the Verifier).

Initialization Alice publishes a (copy of) an angle Y_A, which is constructed by Alice as the triple of an angle X_A she has constructed at random. Because trisecting an angle is impossible, Alice is confident that she is the only one who knows X_A.

Identification Protocol

This has the standard form of an iterated "atomic" three-round protocol:

1. Alice gives Bob a copy of an angle R, which she has constructed as the triple of an angle K that she has selected at random.
2. Bob flips a coin, and tells Alice the result.
3. If Bob says "heads," Alice gives Bob a copy of the angle K and Bob checks that $3 * K = R$. If Bob says "tails," Alice gives Bob a copy of the angle $L = K + X_A$, and Bob checks that $3 * L = R + Y_A$.

The three steps are repeated t-times independently. Bob accepts Alice's proof of identity only if all t checks are successful.

This protocol is an interactive proof of knowledge of the angle X_A (the identity of Alice) with error 2^{-t}. The protocol is also zero-knowledge. Below we sketch a simplified proof for this (a formal proof can easily be obtained by using the approach in [5]).

If Alice and Bob follow the protocol then clearly Bob will always accept Alice's proof of identity. However an imposter, who does not know the secret angle X_A, cannot construct both the angles K and L in step 3 (otherwise he could construct $L - K = X_A$). Thus Bob will accept with probability no better than $1/2$ for each iteration, and no better than 2^{-t} for the t iterations.[1] It follows that the protocol is proof of knowledge of X_A [6].

Next we show that the protocol is zero-knowledge. That is, it is possible to simulate Bob's "view" during the execution of the protocol. Now Bob "sees" the messages of Alice and his own coin flips. The transcripts of these are of type $(R, \text{"heads"}, K)$ or $(R, \text{"tails"}, L)$. To simulate the former, select the angle K at random and take $R = 3 * K$; for the latter, select the angle L at random and solve $3 * L = R + Y_A$ for R.[2] So Bob can simulate his interaction with Alice, and therefore gains zero knowledge about X_A.

We feel that this protocol is simple and clear enough that it forms an excellent pedagogical example of a zero-knowledge identification protocol, such as may be used for high-school students. For a general discussion on interactive proofs, zero-knowledge and identification schemes the reader is referred to [7, 5, 6].

3 Security – the model and background

The goal with the classical constructions is to find a theoretical solution to geometrical problems by using a ruler and a compass, assuming that these have perfect precision. The difficulty of finding solutions is not an issue: if a problem cannot be solved by ruler and compass then this is because there is no solution with these tools (and not because it is hard to find one). We stress that with geometrical constructions the ruler should be a simple straight-edge, and cannot be used for marking distances.

[1] Formally, the knowledge of the prover is checked by an "extractor" M. If a prover succeeds in convincing the verifier with probability greater than the error 2^{-t}, then M can extract X_A (or an equivalent geometric object) by "probing and resetting" the prover [5]. With geometric cryptography there are no complexity bounds on M.

[2] Bob may use a non-uniform distribution. The following proceedure is used to simulate Bob's view [6]. Suppose that the transcripts of $r < t$ rounds have been simulated. Flip a fair coin and construct the corresponding transcript. Give this to Bob and get his coin flip. If this is the same, append the transcript to the list and proceed to the next round. Otherwise "reset" Bob to "his state at the beginning of the r-th round" and repeat the trial. Halt when all rounds are simulated. The expected number of trials for this simulation $2t$. If the protocol is executed in parallel (as in Section 4), then the expected number of trials is 2^t.

3.1 Galois extension fields and impossibility proofs

Analytic geometry provides us with the means to associate the quantitative aspects of geometrical objects (line segments, angles, etc) with real numbers (Desargues). We choose a coordinate system, and the points are represented by pairs (x, y) of reals. In particular, ruler and compass operations will generate points whose coordinates are in number fields $Q' = Q(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n$ are roots of quadratic extensions of the rationals Q (Galois). We call the roots, *radicals*. For example $3\sqrt{5} + 2\sqrt{6 - \sqrt{7}}$ is an element of Q' with radicals $\sqrt{5}$, $\sqrt{7}$, $\sqrt{6 - \sqrt{7}}$.

Let Y be an angle to be trisected and $Q(\cos Y)$ the field of all rational functions of $\cos Y$ over Q (that is, numbers of type $f(\cos Y)/g(\cos Y)$, where f, g are rational polynomials). ¿From trigonometry, $\cos Y = 4\cos^3 \frac{Y}{3} - 3\cos \frac{Y}{3}$. Then the angle Y can be trisected by ruler and compass only if,

$$\cos Y \;=\; 4x^3 - 3x \tag{1}$$

has a solution x in some extension field of $Q(\cos Y)$ with radicals $a_1, \ldots, a_n$. It follows that $\cos Y$ must satisfy an algebraic equation over $Q(a_1, \ldots, a_n)$ which is not trivial.[3] Therefore $\cos Y$ is an algebraic number, and the set of angles which can be trisected is a subset of the reals which has measure zero. Hence almost all angles Y cannot be trisected.

A similar argument applies for the non constructibility of $\sqrt[3]{2}$ (doubling the cube), and more generally the non constructibility $\sqrt[3]{x}$, where x is the length of randomly selected line segment. It follows that the operation of taking cubic powers of the lengths is also a one-way function.

3.2 Random geometrical objects

Geometric constructions often involve selections of arbitrary geometrical objects (for example when constructing the midpoint of a line segment one uses an arbitrary circumference). In such cases it is normally understood that the corresponding numbers are in extensions of the rationals Q with radicals. If an angle X is chosen this way, then the angle $Y = 3 * X$ can be trisected by ruler and compass (in this case equation (1) has the solution $x = \cos X$, with $\cos X$ a rational expression with radicals).

The angle K (and X_A) used in the identification protocol is not constructable by ruler and compass because it was chosen at random in the unit circle of the real plane. Consequently, $\cos K$ does not belong to any extension field of Q with radicals, and the angle $3 * K$ cannot be trisected by ruler and compass given all previous constructions except K, as pointed out in the previous section.

3.3 Historical background

According to the Pythagorean doctrine, the *number* (that is, the rational number) was the essence of all things. Mathematics, philosophy and physics, were all based on numbers. Pythagoras himself may not have been aware of the irrationality of $\sqrt{2}$, but his followers did discover it. This must have caused them considerable consternation, and was kept secret for some time (irrational = $\alpha\lambda o\gamma o\varsigma$, which, according to some scholars means, *unutterable*). It was said that Hippasus, the first Pythagorean to divulge the unutterable, was thrown off a ship and so perished [2]. The school however overcame this setback and later, according to Euclid, was the first school to develop a general theory of irrationality [2].

[3] For ruler and compass constructions such as angle bisections, this equation is trivial: only radicals are involved, and these cancel out.

In the 5th and 4th centuries BC there was a proliferation of geometrical constructions and theorems, many of which overlapped or were flawed. It became necessary to organize these results in some way. Tradition has it that Plato insisted that this task be based on ruler and compass constructions. This approach was adopted by Euclid in his treatise on the *Elements* of geometry.

One of the most famous classical problems is "squaring the circle". Other such problems are "doubling the cube" and trisecting a general angle. More than a century ago it was shown that these problems cannot be solved by ruler and compass (alone). Recently Peter Neumann proved that Ptolemy's spherical mirror problem (finding the point on a sperical mirror where a ray is reflected from a source to an observer) cannot be solved by ruler and compass [8].

For a general discussion on this topic the reader is referred to [7, 1, 3].

4 Extensions of the identification protocol and other applications

Many conventional cryptographic constructions can be replicated in geometrical cryptography. Here we consider some of these, starting with two extensions of the identification protocol in Section 2. The first extension is a parallel execution. The second, a "multiple-secret" version.

For the parallel execution, the t iterations of the protocol are performed at the same time: Alice gives Bob t copies of the angles R_i (step 1), Bob flips t coins (step 2), and finally Alice gives Bob t copies of appropriate angles (step 3). The expected number of trials to simulate this execution is 2^t (see Footnote 2). Since there are no complexity bounds with ruler and compass constructions, the protocol can be simulated. Therefore the parallel execution of the identification protocol is also zero-knowledge. This is in contrast with conventional cryptography, for which it is not known if parallel executions of zero-knowledge protocols are zero-knowledge.

Next we consider a multiple-secret identification protocol. For this, Alice selects k random angles $X_{A,1}, X_{A,2}, \ldots, X_{A,k}$, and publishes their triples $Y_{A,1}, Y_{A,2}, \ldots, Y_{A,k}$. Then Alice proves to Bob that she knows *all* k angles $X_{A,1}, X_{A,2}, \ldots, X_{A,k}$, by using the following three-round protocol, which is repeated t times independently.

1. Alice gives Bob a copy of an angle R, constructed as the triple of a random angle K.
2. Bob gives Alice the bit string $b_1, b_2, \ldots, b_k$ which is determined by k coin flips (0 is "heads", 1 is "tails").
3. Alice gives Bob a copy of the angle $L = K + \sum_{i=1}^{i=k} b_i X_{A,i}$, and Bob checks that $3 * L = R + \sum_{i=1}^{i=k} b_i Y_{A,i}$.

Bob accepts only if the checks are valid for all t iterations. For this protocol the error is 2^{-kt}.

4.1 An authentication protocol

The identification protocol in Section 2 can easily be modified to get an authentication protocol. Let m be the message which Alice wants to authenticate. We require that the message be an integer. This constraint is not very restrictive and, essentially, confines the messages that Alice can authenticate to constructable geometrical objects, since these objects are enumerable.

For the authentication protocol Alice needs two secret angles $X_{A,1}, X_{A,2}$. Alice publishes their triples $Y_{A,1}, Y_{A,2}$. To authenticate m to Bob, Alice proves to Bob that she knows the angle $Z = m * X_{A,1} + X_{A,2}$, by using the identification protocol in Section 2 as follows.

In step 1, Alice gives Bob a copy of the angle R, constructed as the triple of a random angle K. In step 2, Bob flips a coin and tells Alice the outcome as a bit b. Finally in step 3, Alice gives Bob the angle $L = K + b\,(m * X_{A,1} + X_{A,2})$, and Bob checks that $3 * L = R + b\,(m * Y_{A,1} + Y_{A,2})$.

4.2 Adding usable structure to geometric constructions

Let N be an additional angle. We can use N as a modulus when adding or subtracting angles with ruler and compass constructions. Suppose that Y is an angle which is to be trisected modulo N. There are three solutions to the equation $Y = 3 * X \bmod N$ in X, which differ by multiples of $N/3$. Anyone who knows two different solutions X_1, X_2 can therefore trisect the modulus N. This property makes it possible to replicate many of the cryptographic constructions we use in number theory, where knowledge of two different square roots of a number y modulo a number n can lead to the factorization of n. Here is one such application.

Suppose that the distribution of the random points in Axiom 5 is not uniform. Then the identification protocol in Section 2 may fail to be zero-knowledge, because it may not be possible to simulate the transcripts $(R, \text{“tails”}, L)$ by selecting L at random and solving $3 * L = R + Y_A$ for R (R may not have the proper distribution). This means that the protocol may “leak” some knowledge to Bob and make it possible for Bob to construct the secret angle X_A of Alice. We shall show have our earlier observation may be used to strengthen the security of the identification protocol when the distribution of the random angles is not uniform.

First we observe that the distribution of the random angles should be continuous. In particular, the probability that any specific angle K is selected should be zero. Otherwise Bob will get both the angles K and $L = K + X_A$, from which he can construct Alice's secret angle X_A. Now suppose that N is an angle that cannot be trisected by either Alice or Bob (*e.g.*, N is selected randomly by a Trusted Center). To protect her secret angle X_A, Alice will give Bob in the identification protocol, *not* absolute angles but angles modulo N. That is, she gives Bob the angle $R \bmod N$ in step 1, and either $K \bmod N$ or $L \bmod N$ in step 3. This will not turn the distribution of the angles to uniform, but it will destroy any possible discovery by Bob about which of the three trisections of Y_A: X_A, $X_A + N/3$, $X_A + 2N/3$, Alice used in L. Even if Bob were given one of these, he would not know with probability better than $1/3$ whether this was Alice's.

If we assume that this scheme is breakable and that Bob can construct a trisection of Y_A by analyzing the communication, then with probability $2/3$ this trisection will not be the one actually used by Alice. Therefore it will lead with reasonable probability to an impossible trisection of the angle N.

A similar technique was used to prove the security of parallel execution of the Fiat-Shamir identification protocol [5], which is not known to be zero knowledge.

5 Discussion and Conclusions

We suggest that the field of geometric cryptography may be a fruitful one for further study, as it may yield both illuminating examples and insight into cryptographic fundamentals.

We leave as interesting open problems the development of other primitives of geometric cryptography, such as secure encryption techniques or secure signature schemes. (We note that Rompel's proof [4] that “one-way functions are necessary and sufficient for secure signatures” may not apply here, since his proof depends upon the binary representation of messages and ciphertexts.)

Acknowledgments

We dedicate this paper to Jose Pastor, who organized a marvelous gala dinner at Eurocrypt '96, at which dinner this research began.

References

[1] R. Courant and H. Robbins. What is Mathematics? An elementary approach to ideas and methods, Oxford University Press, 1943.

[2] T. Heath. A History of Greek Mathematics, Vol 1, Oxford University Press, 1921.

[3] *The New Encyclopædia Brittanica*, Volume 19, Geometry, pages 887–936, 1995.

[4] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proc. 22nd ACM Symp. on Theory of Computing*, ACM, Baltimore, Maryland, 1990, pages 387–394.

[5] U. Feige, A. Fiat and A. Shamir. Zero Knowledge Proofs of Identity, *Journal of Cryptology*, Vol 1, pages 77–94, 1988.

[6] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *Siam J. Comput.*, Vol 18 (1), pages 186–208, 1989.

[7] J-J Quisquater, L. Guillou, et al. How to explain Zero-Knowledge Protocols to Your Children. In *Advances in Cryptology – Crypto '89*, Lecture Notes in Computer Science #435, G. Brassard ed., Springer-Verlag, Berlin 1990, pages 628–631.

[8] The Daily Telegraph. University don solves the last puzzle left by the Greeks. April 1, 1997.