Understanding patent incentives

Daniel J. Bernstein

1. Examples of patents

2. Examples of cryptographic patents

An example of a patent

British kings and queens issued two types of declarations:

- “Letters close”: private declarations.
- “Letters patent”: public declarations.

An example of a patent

British kings and queens issued two types of declarations:

- “Letters close”: private declarations.
- “Letters patent”: public declarations.

1576: Queen Elizabeth issued a letter patent granting a monopoly to Ralph Bowes and Thomas Bedingfelde.

An example of a patent

British kings and queens issued two types of declarations:

- "Letters close": private declarations.
- "Letters patent": public declarations.

1576: Queen Elizabeth issued a letter patent granting a monopoly to Ralph Bowes and Thomas Bedingfelde. Nobody else was allowed to manufacture, import, or sell playing cards.

An example of a patent

British kings and queens issued two types of declarations:

- “Letters close”: private declarations.
- “Letters patent”: public declarations.

1576: Queen Elizabeth issued a letter patent granting a monopoly to Ralph Bowes and Thomas Bedingfelde. Nobody else was allowed to manufacture, import, or sell playing cards.

1578, 1588: Elizabeth extended the playing-card monopoly.

An example of a patent

British kings and queens issued two types of declarations:

- “Letters close”: private declarations.
- “Letters patent”: public declarations.

1576: Queen Elizabeth issued a letter patent granting a monopoly to Ralph Bowes and Thomas Bedingfelde. Nobody else was allowed to manufacture, import, or sell playing cards.

1578, 1588: Elizabeth extended the playing-card monopoly.

1598: Bowes died. Elizabeth extended the playing-card monopoly and gave it to Edward Darcy “in consideration of his long and acceptable services to the Crown”.

An example of a patent

British kings and queens issued two types of declarations:

- “Letters close”: private declarations.
- “Letters patent”: public declarations.

1576: Queen Elizabeth issued a letter patent granting a monopoly to Ralph Bowes and Thomas Bedingfelde. Nobody else was allowed to manufacture, import, or sell playing cards.

1578, 1588: Elizabeth extended the playing-card monopoly.

1598: Bowes died. Elizabeth extended the playing-card monopoly and gave it to Edward Darcy “in consideration of his long and acceptable services to the Crown”.

Summary of the exchange documented in 1598:
Darcy served queen. Queen gave Darcy a valuable monopoly.

More monopolies granted by Queen Elizabeth

1585: Elizabeth gave Thomas Wilkes a monopoly on salt.
(Wilkes had convinced a German prince to invade France.)

More monopolies granted by Queen Elizabeth

1585: Elizabeth gave Thomas Wilkes a monopoly on salt. (Wilkes had convinced a German prince to invade France.)

Monopolies listed in a 1778 history book: "Currants, salt, iron, powder, cards, calf-skins, fells, pouldavies, ox-shin-bones, train oil, lists of cloth, pot-ashes, anniseeds, vinegar, sea-coals, steel, aquavitae, brushes, pots, bottles, saltpetre, lead, accidences, oil, calamine stone, oil of blubber, glasses, paper, starch, tin, sulphur, new drapery, dried pilchards, transportation of Iron ordnance, of beer, of horn, of leather, importation of Spanish wool, of Irish yarn: These are but a part of the commodities, which had been appropriated to monopolists. . . . These monopolists were so exorbitant in their demands, that in some places they raised the price of salt, from sixteen-pence a bushel, to fourteen or fifteen shillings."

A monopoly not granted

1589: William Lee invented a stocking frame knitting machine.

A monopoly not granted

1589: William Lee invented a stocking frame knitting machine.

Elizabeth didn't grant a patent monopoly.
Why not? Various sources give incompatible stories:

- She wasn't impressed with the knitting quality.
- She was so impressed with the knitting quality that she was worried about destroying the hand-knitting industry.

A monopoly not granted in England

1589: William Lee invented a stocking frame knitting machine.

Elizabeth didn't grant a patent monopoly.
Why not? Various sources give incompatible stories:

- She wasn't impressed with the knitting quality.
- She was so impressed with the knitting quality that she was worried about destroying the hand-knitting industry.

1608: Lee moved to France, where King Henry IV agreed to grant a patent monopoly.

“The Case of Monopolies”

1602: Darcy sued an unauthorized playing-card manufacturer.

One of Darcy’s lawyers, Edward Coke, published a report on the case, although only in 1615.

“The Case of Monopolies”

1602: Darcy sued an unauthorized playing-card manufacturer.

One of Darcy’s lawyers, Edward Coke, published a report on the case, although only in 1615.

Arguments for the patent: “Because the said playing Cards were not any merchandize, or thing concerning Trade of any necessary use, but things of vanity, and the occasion of expence of time, wasting of patrimonies, and of the livings of many, the loss of the service and work of servants, causes of want, which is the mother of wo and perdition, and therefore it belongeth to the Queen . . . to take away the great abuse, and to take order for the moderate and convenient use of them.”

Arguments for the patent, continued

"In matters of recreation and pleasure the Queen hath a Prerogative given her by the Law to take such order for such moderate use of them as shall seem good to her. . . . The Queen in regard of the great abuse of them, and of the deceit of the subjects by reason of them might utterly suppress them, and by consequence without injury to any one, she might moderate and suffer them at her pleasure. And the reason of the Law which giveth the King these Prerogatives in matters of recreation and pleasure was, because the greatest part of men are ready to exceed in them. . . . no subject can make a Park, Chase, or Warren within his own Land, for his recreation or pleasure without the Kings grant or license . . . The King granted to another all the wild Swans betwixt London Brig and Oxford."

The patent monopoly was invalidated

Unanimous decision of the judges: The patent is “a Monopoly, and against the Common Law”, and “against divers Acts of Parliament”.

“The sole Trade of any Mechanical Artifice, or any other Monopoly is not only a damage and prejudice to those who exercise the same Trade, but also to all other subjects, for the end of all these Monopolies is for the private gain of the Patentees . . . after a Monopoly granted, the Commodity is not so good and merchantable as it was before; for the patentee having the sole trade, regardeth only his private, and not the publicke weale.”

Patent monopolies, continued

Example from 1617: King James gave a monopoly on hotels to Giles Mompesson, because of family connections.

Patent monopolies, continued

Example from 1617: King James gave a monopoly on hotels to Giles Mompesson, because of family connections.

Mompesson took bribes from thousands of hotels and bars.

Patent monopolies, continued

Example from 1617: King James gave a monopoly on hotels to Giles Mompesson, because of family connections.

Mompesson took bribes from thousands of hotels and bars.

February 1621: Parliament started investigating Mompesson for extortion.

Patent monopolies, continued

Example from 1617: King James gave a monopoly on hotels to Giles Mompesson, because of family connections.

Mompesson took bribes from thousands of hotels and bars.

February 1621: Parliament started investigating Mompesson for extortion.

3 March 1621: Mompesson fled to France.

Parliament then sentenced Mompesson to life imprisonment, although Prince Charles reduced the sentence.

The “Statute of Monopolies”

12 March 1621: A bill (written by Coke) was introduced in Parliament to outlaw monopolies.

The “Statute of Monopolies”

12 March 1621: A bill (written by Coke) was introduced in Parliament to outlaw monopolies.

George Calvert, Secretary of State, asked for an exception for “new inventions”.

The "Statute of Monopolies"

12 March 1621: A bill (written by Coke) was introduced in Parliament to outlaw monopolies.

George Calvert, Secretary of State, asked for an exception for "new inventions".

1623: Parliament passed "An Act concerning Monopolies and Dispensations with Penal Laws, and the Forfeitures thereof".

Section 1 of the law: All monopolies are invalid.

The “Statute of Monopolies”

12 March 1621: A bill (written by Coke) was introduced in Parliament to outlaw monopolies.

George Calvert, Secretary of State, asked for an exception for “new inventions”.

1623: Parliament passed “An Act concerning Monopolies and Dispensations with Penal Laws, and the Forfeitures thereof”.

Section 1 of the law: All monopolies are invalid.

Exception, Section 6: OK to grant a 14-year monopoly for a “manner of new manufactures” to the “true and first inventor” as long as this does not raise prices or damage trade.

The "Statute of Monopolies"

12 March 1621: A bill (written by Coke) was introduced in Parliament to outlaw monopolies.

George Calvert, Secretary of State, asked for an exception for "new inventions".

1623: Parliament passed "An Act concerning Monopolies and Dispensations with Penal Laws, and the Forfeitures thereof".

Section 1 of the law: All monopolies are invalid.

Exception, Section 6: OK to grant a 14-year monopoly for a "manner of new manufactures" to the "true and first inventor" as long as this does not raise prices or damage trade.

Hmmm. If the second inventor is a year later, the monopoly raises prices for 13 years! The exception is internally consistent only if the second inventor is $\geq$14 years later.

An example of current patent law

The U.S. constitution gives the legislature power to “promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries”.

An example of current patent law

The U.S. constitution gives the legislature power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries".

U.S. patent law says that "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor" unless the "invention" was already available to the public earlier, or was already obvious.

An example of current patent law

The U.S. constitution gives the legislature power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries".

U.S. patent law says that "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor" unless the "invention" was already available to the public earlier, or was already obvious.

Sometimes courts say that "Progress" requires further limits: e.g., patents on "abstract ideas" are prohibited. But courts don't allow arguments saying patent X damages progress.

An example of current patent law

The U.S. constitution gives the legislature power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries".

U.S. patent law says that "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor" unless the "invention" was already available to the public earlier, or was already obvious.

Sometimes courts say that "Progress" requires further limits: e.g., patents on "abstract ideas" are prohibited. But courts don't allow arguments saying patent X damages progress.

The U.S. patent office is paid for each patent it grants.

Another example of current patent law

The European Patent Convention says that “European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application”.

Another example of current patent law

The European Patent Convention says that "European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application".

Exception: does not permit patents on "mathematical methods", "mental acts", "programs for computers", etc. However, no general requirement to promote progress.

Another example of current patent law

The European Patent Convention says that “European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application”.

Exception: does not permit patents on “mathematical methods”, “mental acts”, “programs for computers”, etc. However, no general requirement to promote progress.

European patent offices are paid for each patent they grant.

How to pretend that patents promote progress

Typical patent advertising, for various choices of X:

1. Observe that X was patented: a monopoly was granted on X, in exchange for making X public.
2. Observe that deployment of X has societal value.
3. Conclude that the patent on X has societal value.

How to pretend that patents promote progress

Typical patent advertising, for various choices of X:

1. Observe that X was patented: a monopoly was granted on X, in exchange for making X public.
2. Observe that deployment of X has societal value.
3. Conclude that the patent on X has societal value.
4. Don't ask whether X would have been published without the patent.
5. Don't ask whether X would have had *more* deployment and *more* societal value without the patent.

“This wouldn’t have been invented without me!”

Mark Lemley, “The myth of the sole inventor”, 2012: “The theory of patent law is based on the idea that a lone genius can solve problems that stump the experts, and that the lone genius will do so only if properly incented. But the canonical story of the lone genius inventor is largely a myth. Surveys of hundreds of significant new technologies show that almost all of them are invented simultaneously or nearly simultaneously by two or more teams working independently of each other.”

1. Examples of patents

2. Examples of cryptographic patents

Public-key cryptography

Summer 1975: Ralph Merkle submitted a paper "Secure communications over insecure channels" describing a public-key system (the puzzles system).

Public-key cryptography

Summer 1975: Ralph Merkle submitted a paper "Secure communications over insecure channels" describing a public-key system (the puzzles system).

December 1975: Whitfield Diffie and Martin Hellman, independently of Merkle, distributed a paper "Multiuser cryptographic techniques" describing various public-key systems (e.g., permuted circuits). "We wrote the paper in December 1975 and sent preprints around immediately."

This was before the "New directions in cryptography" paper.

Searching for public-key cryptosystems

Some candidate one-way functions that Diffie considered:

- John Gill had suggested exponentiation.
- Diffie had checked a survey of NP-complete problems and had selected “knapsacks”.
- Donald Knuth had suggested $p, q \mapsto pq$.

Diffie, Hellman, Knuth, and Gill were all at Stanford.
People elsewhere also started searching for examples when they learned about public-key cryptography: see, e.g., RSA.

Exponential key exchange

Hellman wrote down exponential key exchange “early one morning in May 1976”.

Diffie says he and Hellman “hastened to add it to both the upcoming National Computer Conference presentation and to ‘New Directions’ . . . It was sent off to the IEEE Transactions on Information Theory prior to my departure for NCC and like all of our other papers was immediately circulated in preprint.”

June 1976: Diffie and Hellman presented exponential key exchange at the National Computer Conference in Massachusetts and at another conference in Sweden.

No thoughts of patents

2001 Steven Levy book, based on interviews: in 1976, "thoughts about exploiting intellectual property were the furthest thing from the minds of these information scientists. In contrast to what struck them as a government refusal to provide all the details of the Data Encryption Standard, they were creating a fully open alternative to conventional cryptography itself."

Stanford: Hey, look, we can make money!

September 1977: Stanford filed a patent application on public-key cryptography and specifically on exponential key exchange.

Stanford: Hey, look, we can make money!

September 1977: Stanford filed a patent application on public-key cryptography and specifically on exponential key exchange.

Regarding 1975 paper presenting public-key cryptography, the Stanford lawyers falsely claimed that the 1975 paper didn't present a "demonstration system".

Stanford: Hey, look, we can make money!

September 1977: Stanford filed a patent application on public-key cryptography and specifically on exponential key exchange.

Regarding 1975 paper presenting public-key cryptography, the Stanford lawyers falsely claimed that the 1975 paper didn't present a "demonstration system".

Regarding June 1976 paper+talk presenting exponential key exchange, the Stanford lawyers misled the patent office into believing that the paper was first available in "*IEEE Transactions on Information Theory* . . . Nov. 1976".

Stanford: Hey, look, we can make money!

September 1977: Stanford filed a patent application on public-key cryptography and specifically on exponential key exchange.

Regarding 1975 paper presenting public-key cryptography, the Stanford lawyers falsely claimed that the 1975 paper didn't present a "demonstration system".

Regarding June 1976 paper+talk presenting exponential key exchange, the Stanford lawyers misled the patent office into believing that the paper was first available in "*IEEE Transactions on Information Theory* . . . Nov. 1976".

U.S. allows you to publish X, wait a year, and then file a patent application on X. (Many countries don't allow this: you already published, so why should we give you a patent?)

Patent damaged DH deployment for 20 years

Hellman–Diffie–Merkle received US patent 4200770 in 1980.
Claim 1: the entire concept of public-key encryption.
Claim 6: DH exponential key exchange.

Patent damaged DH deployment for 20 years

Hellman–Diffie–Merkle received US patent 4200770 in 1980.
Claim 1: the entire concept of public-key encryption.
Claim 6: DH exponential key exchange.

Patent-holding company, Public Key Partners, claimed that "all known methods of practicing the art of Public Key" were covered by this and followup patents.

Patent damaged DH deployment for 20 years

Hellman–Diffie–Merkle received US patent 4200770 in 1980.
Claim 1: the entire concept of public-key encryption.
Claim 6: DH exponential key exchange.

Patent-holding company, Public Key Partners, claimed that "all known methods of practicing the art of Public Key" were covered by this and followup patents.

A court case was filed in 1994 saying the patent was invalid. Case filings then provided detailed evidence of DH paper being distributed more than a year before patent filing. The case was privately settled in 1997. The patent expired in 1997.

RSA, Rabin, etc.

Ronald Rivest, Adi Shamir, and Leonard Adleman, assistant professors at MIT, wrote an April 1977 technical report on their cryptosystem, and discussed the cryptosystem with Martin Gardner for publication in his Scientific American column in August 1977.

RSA, Rabin, etc.

Ronald Rivest, Adi Shamir, and Leonard Adleman, assistant professors at MIT, wrote an April 1977 technical report on their cryptosystem, and discussed the cryptosystem with Martin Gardner for publication in his Scientific American column in August 1977.

1978 Michael Rabin, "Digitalized signatures", page 156: a public-key system "employing large prime numbers was discovered by the author (unpublished) and independently by Rivest, Adleman and Shamir [3]".

RSA, Rabin, etc.

Ronald Rivest, Adi Shamir, and Leonard Adleman, assistant professors at MIT, wrote an April 1977 technical report on their cryptosystem, and discussed the cryptosystem with Martin Gardner for publication in his Scientific American column in August 1977.

1978 Michael Rabin, "Digitalized signatures", page 156: a public-key system "employing large prime numbers was discovered by the author (unpublished) and independently by Rivest, Adleman and Shamir [3]".

Remember also Knuth suggesting $p, q \mapsto pq$ as one-way.

MIT: We can make money too!

August 1977 column from Gardner said tech report was available from Rivest. Rivest sent out thousands of copies.

MIT: We can make money too!

August 1977 column from Gardner said tech report was available from Rivest. Rivest sent out thousands of copies.

Simson Garfinkel's PGP book, page 78: the "head of the MIT Laboratory for Computer Science reviewed the RSA research and decided that the algorithm might be patentable".

MIT: We can make money too!

August 1977 column from Gardner said tech report was available from Rivest. Rivest sent out thousands of copies.

Simson Garfinkel's PGP book, page 78: the "head of the MIT Laboratory for Computer Science reviewed the RSA research and decided that the algorithm might be patentable".

December 1977: MIT filed RSA patent application. Garfinkel: "since the algorithm had been published before the patent application was filed, MIT could not secure foreign rights to the invention."

Patent damaged RSA deployment for 23 years

Rivest–Shamir–Adleman received US patent 4405829 in 1983.

Garfinkel, page 100: "Bidzos' most effective weapon against the organized distribution of PGP was the RSA patent. Whenever Bidzos learned of an organization that was distributing copies of PGP, he wrote it letters demanding that it stop. CompuServe and America Online were both forced to take copies of PGP off their systems. Bidzos also went after universities, demanding that they not make PGP available to their students. According to Rotenberg, even the esteemed EFF took PGP off its FTP site."

Patent expired in 2000.

These patents did not promote progress

Public-key cryptography, exponential key exchange, and RSA were published as a result of the usual academic publication incentives—credit is assigned to the first to publish—before the authors thought about patenting them.

These patents did not promote progress

Public-key cryptography, exponential key exchange, and RSA were published as a result of the usual academic publication incentives—credit is assigned to the first to publish—before the authors thought about patenting them.

Also: There were two independent discoveries of public-key cryptography, and two independent discoveries of RSA. Presumably, if Gill and DH hadn't discovered exponential key exchange, other academics would have soon discovered it.

The Schnorr patent

1989: Claus Schnorr, professor at the University of Frankfurt,
filed a patent application on a signature system,
more streamlined than earlier signature systems.
In particular, shorter signatures for $\mathbb{F}_p^*$,
although same-length signatures for $E(\mathbb{F}_p)$.

The Schnorr patent

1989: Claus Schnorr, professor at the University of Frankfurt,
filed a patent application on a signature system,
more streamlined than earlier signature systems.
In particular, shorter signatures for $\mathbb{F}_p^*$,
although same-length signatures for $E(\mathbb{F}_p)$.

February 1991: Schnorr received U.S. patent 4995082.
Schnorr also received patents in other countries later.

The Schnorr patent

1989: Claus Schnorr, professor at the University of Frankfurt,
filed a patent application on a signature system,
more streamlined than earlier signature systems.
In particular, shorter signatures for $\mathbb{F}_p^*$,
although same-length signatures for $E(\mathbb{F}_p)$.

February 1991: Schnorr received U.S. patent 4995082.
Schnorr also received patents in other countries later.

Public Key Partners bought the patent from Schnorr.

The Schnorr patent

1989: Claus Schnorr, professor at the University of Frankfurt,
filed a patent application on a signature system,
more streamlined than earlier signature systems.
In particular, shorter signatures for $\mathbb{F}_p^*$,
although same-length signatures for $E(\mathbb{F}_p)$.

February 1991: Schnorr received U.S. patent 4995082.
Schnorr also received patents in other countries later.

Public Key Partners bought the patent from Schnorr.

Schnorr patent expired in 2008. Without patents, would it
have taken until 2008 for someone else to discover this system?
Would Schnorr not have published it?

DSA: the Digital Signature Algorithm

August 1991: NIST issued a Federal Register notice announcing a proposed Digital Signature Standard.

DSA: the Digital Signature Algorithm

August 1991: NIST issued a Federal Register notice announcing a proposed Digital Signature Standard.

August 1991: Computer Professionals for Social Responsibility filed a Freedom of Information Act request.

October 1991: CPSR appealed FOIA denial.

April 1992: CPSR filed a FOIA lawsuit.

DSA: the Digital Signature Algorithm

August 1991: NIST issued a Federal Register notice announcing a proposed Digital Signature Standard.

August 1991: Computer Professionals for Social Responsibility filed a Freedom of Information Act request.

October 1991: CPSR appealed FOIA denial.

April 1992: CPSR filed a FOIA lawsuit.

June 1992: FOIA response admitted that there were 142 pages from NIST + 1138 from NSA.

April 1993: FOIA documents indicated that NSA had dominated the DSA design.

The DSA patent

July 1991: NIST secretly filed a U.S. patent application on DSA, listing NSA's David Kravitz as inventor.

June 1992: NIST secretly filed patent applications on DSA in CA, HU, NL, JP, WO, AU, BR, EP, SE, FI, NO.

The DSA patent

July 1991: NIST secretly filed a U.S. patent application on DSA, listing NSA's David Kravitz as inventor.

June 1992: NIST secretly filed patent applications on DSA in CA, HU, NL, JP, WO, AU, BR, EP, SE, FI, NO.

June 1993: NIST announced that it had a patent application and would transfer the patent to Public Key Partners "unless, within sixty (60) days of this notice, NIST receives written evidence and argument which established that the grant of the license would not be consistent with" the law.

The DSA patent

July 1991: NIST secretly filed a U.S. patent application on DSA, listing NSA's David Kravitz as inventor.

June 1992: NIST secretly filed patent applications on DSA in CA, HU, NL, JP, WO, AU, BR, EP, SE, FI, NO.

June 1993: NIST announced that it had a patent application and would transfer the patent to Public Key Partners "unless, within sixty (60) days of this notice, NIST receives written evidence and argument which established that the grant of the license would not be consistent with" the law.

July 1993: NIST received U.S. patent 5231668.

NIST's excuse for the giveaway

NIST claimed that its goal was to "minimize royalties".

NIST admitted that transferring the patent to PKP "would allow PKP to collect royalties on the DSS for the remainder of the government 17-year patent term (i.e., until 2010)".

NIST's excuse for the giveaway

NIST claimed that its goal was to "minimize royalties".

NIST admitted that transferring the patent to PKP "would allow PKP to collect royalties on the DSS for the remainder of the government 17-year patent term (i.e., until 2010)".

NIST's counterarguments:

- The Schnorr patent wouldn't expire until 2008 anyway.
- The transfer would avoid litigation.
- "PKP's royalty rates for the right to make or sell products, subject to uniform minimum fees, will be no more than 2 1/2% for hardware products and 5% for software".

Stopping the DSA patent giveaway

In fact, PKP's "uniform minimum fees" were

- $10,000/$25,000 for small/large companies, plus
- $10,000 per program per year, plus
- $5 per program per user after 2000 users.

Cheaper for each company than a patent lawsuit,
but clearly not compatible with widespread usage of signatures.

Stopping the DSA patent giveaway

In fact, PKP's "uniform minimum fees" were

- $10,000/$25,000 for small/large companies, plus
- $10,000 per program per year, plus
- $5 per program per user after 2000 users.

Cheaper for each company than a patent lawsuit,
but clearly not compatible with widespread usage of signatures.

July 1993: I distributed (1) a form letter requesting a free non-exclusive DSA license from NIST and (2) a letter objecting to NIST's transfer of DSA to PKP.

Stopping the DSA patent giveaway

In fact, PKP's "uniform minimum fees" were

- $10,000/$25,000 for small/large companies, plus
- $10,000 per program per year, plus
- $5 per program per user after 2000 users.

Cheaper for each company than a patent lawsuit,
but clearly not compatible with widespread usage of signatures.

July 1993: I distributed (1) a form letter requesting a free non-exclusive DSA license from NIST and (2) a letter objecting to NIST's transfer of DSA to PKP.

1994: NIST gave up on the transfer to PKP, and issued the DSA standard with a claim that NIST "is not aware of any patents that would be infringed by this standard".

Fast primes for ECC

Paper by Andreas Bender and Guy Castagnoli at Crypto 1989 reported an implementation of DH on various elliptic curves, including an elliptic curve mod $2^{127} + 24933$, "which is convenient in computer arithmetic."

Fast primes for ECC

Paper by Andreas Bender and Guy Castagnoli at Crypto 1989 reported an implementation of DH on various elliptic curves, including an elliptic curve mod $2^{127} + 24933$, “which is convenient in computer arithmetic.”

1991: Richard Crandall filed patent applications on ECDH over $\mathbb{F}_p$ “where p is one of a class of numbers such that mod p arithmetic is performed in a processor using only shift and add operations”; specifically with $p = 2^q - C$ for C below 32 bits; specifically with $p = 2^q - 1$; specifically with $p = 2^q + 1$; etc.

Fast primes for ECC

Paper by Andreas Bender and Guy Castagnoli at Crypto 1989 reported an implementation of DH on various elliptic curves, including an elliptic curve mod $2^{127} + 24933$, “which is convenient in computer arithmetic.”

1991: Richard Crandall filed patent applications on ECDH over $\mathbb{F}_p$ “where p is one of a class of numbers such that mod p arithmetic is performed in a processor using only shift and add operations”; specifically with $p = 2^q - C$ for C below 32 bits; specifically with $p = 2^q - 1$; specifically with $p = 2^q + 1$; etc.

Crandall received U.S. patents 5159632, 5271061, 5463690.

Fast exponentiation

Andrew Yao and Nicholas Pippenger published various exponentiation algorithms in 1976. Knuth published slight improvements to Yao's algorithm in 1981.

Fast exponentiation

Andrew Yao and Nicholas Pippenger published various exponentiation algorithms in 1976. Knuth published slight improvements to Yao's algorithm in 1981.

Ernest Brickell, Daniel Gordon, Kevin McCurley, and David Wilson published algorithms at Eurocrypt 1992 that are actually the same as

- Knuth's algorithm and
- an example of Pippenger's algorithm.

Fast exponentiation

Andrew Yao and Nicholas Pippenger published various exponentiation algorithms in 1976. Knuth published slight improvements to Yao's algorithm in 1981.

Ernest Brickell, Daniel Gordon, Kevin McCurley, and David Wilson published algorithms at Eurocrypt 1992 that are actually the same as

- Knuth's algorithm and
- an example of Pippenger's algorithm.

Brickell–Gordon–McCurley received U.S. patent 5299262.

Fast exponentiation

Andrew Yao and Nicholas Pippenger published various exponentiation algorithms in 1976. Knuth published slight improvements to Yao's algorithm in 1981.

Ernest Brickell, Daniel Gordon, Kevin McCurley, and David Wilson published algorithms at Eurocrypt 1992 that are actually the same as

- Knuth's algorithm and
- an example of Pippenger's algorithm.

Brickell–Gordon–McCurley received U.S. patent 5299262.

Pil-Joong Lee and Chae-Hoon Lim received U.S. patent 5999627 on an improvement of the 1992 paper.
This is still an example of Pippenger's algorithm.

Compressing elliptic-curve points

Greg Harper, Alfred Menezes, and Scott Vanstone, Eurocrypt 1992: “The key length can be shortened to $n+1$ bits as follows. . . . Thus to transmit P it is sufficient to transmit $\overline{x}$ and the least significant bit of $\overline{y}/\overline{x}$.”

Compressing elliptic-curve points

Greg Harper, Alfred Menezes, and Scott Vanstone, Eurocrypt 1992: "The key length can be shortened to $n+1$ bits as follows. . . . Thus to transmit P it is sufficient to transmit $\overline{x}$ and the least significant bit of $\overline{y}/\overline{x}$."

Vanstone, Ronald Mullin, and Gordon Agnew filed a patent application in July 1994, and received U.S. patent 6141420.

Compressing elliptic-curve points

Greg Harper, Alfred Menezes, and Scott Vanstone, Eurocrypt 1992: "The key length can be shortened to $n+1$ bits as follows. . . . Thus to transmit P it is sufficient to transmit $\overline{x}$ and the least significant bit of $\overline{y}/\overline{x}$."

Vanstone, Ronald Mullin, and Gordon Agnew filed a patent application in July 1994, and received U.S. patent 6141420.

No mention in the patent application that point compression was already published in 1992. The patent's bibliography includes Menezes's 93-page thesis from 1992; what's the chance a patent examiner would find this and read it?

Certicom damaged ECC deployment for 20 years

Vanstone's company, Certicom, obtained more patents, and sent letters saying it had patents on "point compression, public-key validation, key establishment protocols, implicit certificates, digital signature schemes, . . . speeding up finite-field operations and modular integer arithmetic, . . . "

Certicom sued Sony in 2007. Case settled in 2009.

In fact, state-of-the-art ECC used nothing from Certicom, but many companies needed years to decide ECC was safe.

The mindset of people applying for patents

Easy to understand what the “inventors” are thinking:

- “Maybe patents will give us more money.”
- “Maybe patents will give us more credit.”
- “Maybe our employers will give us patent bonuses.”
- “Why not try it?”

The mindset of people applying for patents

Easy to understand what the “inventors” are thinking:

- “Maybe patents will give us more money.”
- “Maybe patents will give us more credit.”
- “Maybe our employers will give us patent bonuses.”
- “Why not try it?”

Natural consequences of this thought process:

- Look for recently published ideas. File patents on those.

The mindset of people applying for patents

Easy to understand what the "inventors" are thinking:

- "Maybe patents will give us more money."
- "Maybe patents will give us more credit."
- "Maybe our employers will give us patent bonuses."
- "Why not try it?"

Natural consequences of this thought process:

- Look for recently published ideas. File patents on those.
- "Serve" as paper reviewer, looking for ideas to patent.

The mindset of people applying for patents

Easy to understand what the “inventors” are thinking:

- “Maybe patents will give us more money.”
- “Maybe patents will give us more credit.”
- “Maybe our employers will give us patent bonuses.”
- “Why not try it?”

Natural consequences of this thought process:

- Look for recently published ideas. File patents on those.
- “Serve” as paper reviewer, looking for ideas to patent.
- Collaborate on projects, looking for ideas to patent.

Scientists can take action to discourage patents

Journals and conferences can require each reviewer to sign the following: “In exchange for being allowed to participate in this scientific process: (1) I agree that I will not apply for any patents for the next 5 years. (2) I certify that I have not applied for any patents in the previous 5 years. (3) I agree that both of these 5-year periods are extended by an additional year for each patent application that I have ever filed.”

Scientists can similarly require this from collaborators.