Complexity and Cryptography

Thomas Zeugmann

Hokkaido University
Laboratory for Algorithmics

https://www-alg.ist.hokudai.ac.jp/~thomas/COCRB/

Lecture 16: Digital Signatures

Motivation I

We consider two parties A and B with possibly conflicting interests. Typically, the parties could be a bank and its customer, any two parties wishing to do business over the internet, diplomats from countries with different interests, and so on.

Motivation I

We consider two parties A and B with possibly conflicting interests. Typically, the parties could be a bank and its customer, any two parties wishing to do business over the internet, diplomats from countries with different interests, and so on.

If we are doing business on the internet we require security and trust, since we cannot see the person we are dealing with; we cannot see any document proving the partner's identity, and we cannot even know if the web site we are connected to belongs to the society it says.

Motivation I

We consider two parties A and B with possibly conflicting interests. Typically, the parties could be a bank and its customer, any two parties wishing to do business over the internet, diplomats from countries with different interests, and so on.

If we are doing business on the internet we require security and trust, since we cannot see the person we are dealing with; we cannot see any document proving the partner's identity, and we cannot even know if the web site we are connected to belongs to the society it says.

To answer these juridical demands, the European Union adopted a community framework for electronic signatures some time ago (directive 1999/93/EC of the European Parliament and the council of December 13, 1999, on a community framework for electronic signatures) that has been implemented in various European countries.

Motivation II

The European directive is used for business in which European partners (persons or societies) or public administrations are involved. It also means that if a Japanese or an American organization enters into an electronic contract with a European society it has to respect European requirements to ensure the contract is valid.

Motivation II

The European directive is used for business in which European partners (persons or societies) or public administrations are involved. It also means that if a Japanese or an American organization enters into an electronic contract with a European society it has to respect European requirements to ensure the contract is valid.

Japan also has an e-Signature Law that formally took effect in April 2001. We shall focus here on important general requirements. For all details, please study the corresponding laws.

Motivation III

Important: If we copy a conventionally signed document, then there are usually ways for distinguishing the copied document and the original one. But a copy of a signed digital document is *identical* to the original one.

Motivation III

Important: If we copy a conventionally signed document, then there are usually ways for distinguishing the copied document and the original one. But a copy of a signed digital document is *identical* to the original one.

So, if A sends a message to B authorizing B to withdraw 1000 € form A's bank account then the intention is usually that B is doing it once and not all the time B feels the need of getting 1000 €.

Motivation III

Important: If we copy a conventionally signed document, then there are usually ways for distinguishing the copied document and the original one. But a copy of a signed digital document is *identical* to the original one.

So, if A sends a message to B authorizing B to withdraw 1000 € form A's bank account then the intention is usually that B is doing it once and not all the time B feels the need of getting 1000 €.

Since the identity of the digital copy and the digital original cannot be prevented, the *message itself* should contain the necessary information such as a date, the clear statement *once*, and so on.

Motivation IV

A digital signature is usually based on public-key cryptographic systems. European law distinguishes between an electronic signature (also called *weak digital signature*) and an *advanced electronic signature*.

Motivation IV

A digital signature is usually based on public-key cryptographic systems. European law distinguishes between an electronic signature (also called *weak digital signature*) and an *advanced electronic signature*.

Question

Why do we have to distinguish between a weak digital signature and an advanced electronic signature?

Motivation IV

A digital signature is usually based on public-key cryptographic systems. European law distinguishes between an electronic signature (also called *weak digital signature*) and an *advanced electronic signature*.

Question

Why do we have to distinguish between a weak digital signature and an advanced electronic signature?

A weak digital signature is used for *authentication*. That is, such a signature should prove that the person who sent the text is the electronic signature's holder. However, we cannot be sure that the person who sent the message is also the *key owner* (cf. Lecture 14).

Motivation V

The key owner does not only have the means to sign a message appropriately but has also the *explicit right* to use it.

Motivation V

The key owner does not only have the means to sign a message appropriately but has also the *explicit right* to use it.

For seeing the difference, we look at a typical example. Usually a key holder would be a server that creates signatures on, for example, a company's software. The company or employee would be the key owner. So, someone in the company could hack the server and sign something contentious using the company's authority.

Motivation V

The key owner does not only have the means to sign a message appropriately but has also the *explicit right* to use it.

For seeing the difference, we look at a typical example. Usually a key holder would be a server that creates signatures on, for example, a company's software. The company or employee would be the key owner. So, someone in the company could hack the server and sign something contentious using the company's authority.

Also, an electronic signature does not guarantee the *integrity* of the message signed. That is, a third party may have altered the text sent without having changed the signature. Of course, this is usually not what we want. We also want to be sure that the text received is the same that was sent, and that no hacker had changed it.

Motivation VI

To summarize, *authentication* guarantees that the message received, say from A, has been really sent by A. It should be at least very difficult if not impossible for a third party C to pretend to be A.

Integrity guarantees that the message received is the same as the message sent. So, no third party and also not the legal recipient should be able to forge a message and to pretend to have received it in properly signed form from A.

Motivation VI

To summarize, *authentication* guarantees that the message received, say from A, has been really sent by A. It should be at least very difficult if not impossible for a third party C to pretend to be A.

Integrity guarantees that the message received is the same as the message sent. So, no third party and also not the legal recipient should be able to forge a message and to pretend to have received it in properly signed form from A.

Putting these requirements together leads to an *advanced electronic signature*.

Requirements to an advanced electronic signature

(1) it is uniquely linked to the signatory;

(2) it is capable of identifying the signatory;

(3) it is created using means that the signatory can maintain under his sole control; and

(4) it is linked to the data to which it relates such that any subsequent change of the data is detectable.

Requirements to an advanced electronic signature

(1) it is uniquely linked to the signatory;
(2) it is capable of identifying the signatory;
(3) it is created using means that the signatory can maintain under his sole control; and
(4) it is linked to the data to which it relates such that any subsequent change of the data is detectable.

In some sense, these requirements are contradictory. For verifying that the message received is from A, as claimed, B should know at least something about A's signature. For B not being able to manipulate a signed message received from A (or for a third party C aiming the same), neither B nor any third party should know too much about A's signature.

Realizing Advanced Digital Signatures I

So, let us first see how these requirements can be fulfilled simultaneously, at least in principle, when using a public-key cryptosystem.

We denote by $E_A, E_B, \ldots$, and $D_A, D_B, \ldots$, the encryption and decryption algorithms (keys) used by the parties $A, B, \ldots$.

Then the following protocol can be used: Let us assume that A sends a message to B.

Protocol DS

Step 1: First, A applies to message w she wants to send her decryption algorithm D_A obtaining $\widehat{w} = D_A(w)$. Then she computes

$$c = E_B(\widehat{w})$$

and sends c to B.

Step 2: First, B applies D_B to the message c received, i.e., B computes $\hat{c} = D_B(c)$. Then B computes

$$w = E_A(\hat{c})\ .$$

Protocol DS

Step 1: First, A applies to message w she wants to send her decryption algorithm D_A obtaining $\widehat{w} = D_A(w)$. Then she computes

$$c = E_B(\widehat{w})$$

and sends c to B.

Step 2: First, B applies D_B to the message c received, i.e., B computes $\hat{c} = D_B(c)$. Then B computes

$$w = E_A(\hat{c}) \, .$$

Observe that the protocol is correct, since by associativity we have

$$E_A(D_B(E_B(D_A(w)))) = E_A(D_A(w)) = w \, .$$

Properties of Protocol DS

(1) Taking into account that *only* A knows D_A neither B nor a third party C can forge A's signature.

Properties of Protocol DS

(1) Taking into account that *only* A knows D_A neither B nor a third party C can forge A's signature.

(2) A cannot deny having sent the signed message to B, since A is the only one knowing D_A.

Properties of Protocol DS

(1) Taking into account that *only* A knows D_A neither B nor a third party C can forge A's signature.

(2) A cannot deny having sent the signed message to B, since A is the only one knowing D_A.

(3) If the underlying public-key cryptosystem is indeed satisfactory, then the application of D_A changes the whole text and not only the name of the sender A. Thus, even if many messages are exchanged, it seems hard to get some knowledge concerning A's signature.

Properties of Protocol DS – continued

Question I

Why A first applies D_A and then E_B?

Properties of Protocol DS – continued

Question I

Why A first applies D_A and then E_B?

She could also first apply E_B and then D_A. This would require that B is also changing the order of applications, i.e., first E_A and then D_B. Consequently, the protocol would be still correct.

Properties of Protocol DS – continued

Question I

Why A first applies D_A and then E_B?

She could also first apply E_B and then D_A. This would require that B is also changing the order of applications, i.e., first E_A and then D_B. Consequently, the protocol would be still correct.

Question II

Does this mean that we have two possibilities for designing our advanced digital signature scheme?

Answer

For seeing the difference let us assume that C is an eavesdropper.
So, C catches the message from A and makes sure that it is not directly delivered to B.

Answer

For seeing the difference let us assume that C is an eavesdropper.
So, C catches the message from A and makes sure that it is not directly delivered to B.

If we use the second version, then C may herself apply E_A and has now $E_B(w)$. This gives C the possibility to sign the message with her own name by applying D_C to it. If C transmits $D_C(E_B(w))$ to B then B would verify to have received the message from C instead of having received it from A.

Answer

For seeing the difference let us assume that C is an eavesdropper.
So, C catches the message from A and makes sure that it is not directly delivered to B.

If we use the second version, then C may herself apply E_A and has now $E_B(w)$. This gives C the possibility to sign the message with her own name by applying D_C to it. If C transmits $D_C(E_B(w))$ to B then B would verify to have received the message from C instead of having received it from A.

Thus, though the original plaintext remains unchanged the *identity of the sender* (that is A) is gone.

Answer

For seeing the difference let us assume that C is an eavesdropper.
So, C catches the message from A and makes sure that it is not directly delivered to B.

If we use the second version, then C may herself apply E_A and has now $E_B(w)$. This gives C the possibility to sign the message with her own name by applying D_C to it. If C transmits $D_C(E_B(w))$ to B then B would verify to have received the message from C instead of having received it from A.

Thus, though the original plaintext remains unchanged the *identity of the sender* (that is A) is gone.

Because of this potential difficulty, our *Protocol DS* was designed in a way that sending happened before encryption.

Properties of Protocol DS – continued

Our *Protocol DS* has also the advantage that only the legal recipient can read it provided D_B is kept secret. This property is usually referred to as *confidentiality*.

Properties of Protocol DS – continued

Our *Protocol DS* has also the advantage that only the legal recipient can read it provided D_B is kept secret. This property is usually referred to as *confidentiality*.

But still, we have a problem.

Properties of Protocol DS – continued

Our *Protocol DS* has also the advantage that only the legal recipient can read it provided D_B is kept secret. This property is usually referred to as *confidentiality*.

But still, we have a problem.

The *Protocol DS* does not take care of two issues that are very important:
A can still *deny* to have sent the message and B can *deny* to have received it.

Properties of Protocol DS – continued

Our *Protocol DS* has also the advantage that only the legal recipient can read it provided D_B is kept secret. This property is usually referred to as *confidentiality*.

But still, we have a problem.

The *Protocol DS* does not take care of two issues that are very important:
A can still *deny* to have sent the message and B can *deny* to have received it.

In terms of law these two issues are summarized by the term *non-repudiation*.

Undeniable Digital Signature

A digital signature satisfying authentication, integrity, confidentiality and non-repudiation is usually called *strong digital signature* or *undeniable digital signature*.

Undeniable Digital Signature

A digital signature satisfying authentication, integrity, confidentiality and non-repudiation is usually called *strong digital signature* or *undeniable digital signature*.

In order to arrive at undeniable digital signatures, one has to combine the *Protocol DS* with a *challenge response protocol* as described in Lecture 14.

An Undeniable Digital Signature Scheme I

We describe here an undeniable digital signature scheme that was introduced by Chaum and van Antwerpen in 1989. It consists of three components:

- a *signing* algorithm *sig*,
- a *verification protocol*, and
- a *disavowal protocol*.

Again we assume that A sends a message to B.

An Undeniable Digital Signature Scheme I

We describe here an undeniable digital signature scheme that was introduced by Chaum and van Antwerpen in 1989. It consists of three components:

- a *signing* algorithm *sig*,
- a *verification protocol*, and
- a *disavowal protocol*.

Again we assume that A sends a message to B.

The new point is that A's cooperation is required to verify a signature made by the signer A. This protects A against the possibility that documents signed by her are duplicated and distributed electronically without her approval.

An Undeniable Digital Signature Scheme II

Question

But what prevents A from disavowing a signature made by her at an earlier time?

An Undeniable Digital Signature Scheme II

Question

But what prevents A from disavowing a signature made by her at an earlier time?

Participant A might claim that a valid signature is a forgery, and either refuse to verify it, or carry out the verification in a way such that the valid signature will not be verified.

An Undeniable Digital Signature Scheme II

Question

But what prevents A from disavowing a signature made by her at an earlier time?

Participant A might claim that a valid signature is a forgery, and either refuse to verify it, or carry out the verification in a way such that the valid signature will not be verified.

That is the point where the disavowal protocol comes into play. Using this disavowal protocol, A can *prove that a signature not made by her is indeed a forgery*. Now, if A refuses to take part in this disavowal protocol, court will take this as evidence that the signature given has been made by A.

Protocol CvA

Let $p = 2q + 1$ be a prime such that q is prime and the discrete log problem in $\mathbb{Z}_p$ is intractible. Let $\alpha \in \mathbb{Z}_p^*$ be an element of order q. Let $1 \leqslant a \leqslant q - 1$ and define $\beta = \alpha^a \mod p$. Furthermore, by G we denote the multiplicative subgroup of $\mathbb{Z}_p^*$ of order q. Note that G consists of the quadratic residues modulo p.

The values p, α and β are *public* and a is kept *secret* by A.

Protocol CvA

Let $p = 2q + 1$ be a prime such that q is prime and the discrete log problem in $\mathbb{Z}_p$ is intractible. Let $\alpha \in \mathbb{Z}_p^*$ be an element of order q. Let $1 \leqslant a \leqslant q - 1$ and define $\beta = \alpha^a \mod p$. Furthermore, by G we denote the multiplicative subgroup of $\mathbb{Z}_p^*$ of order q. Note that G consists of the quadratic residues modulo p.

The values p, α and β are *public* and a is kept *secret* by A.

The plaintext messages x are assumed to be elements of G and so are the ciphers (as we shall see in a moment).

Protocol CvA

Let $p = 2q + 1$ be a prime such that q is prime and the discrete log problem in $\mathbb{Z}_p$ is intractible. Let $\alpha \in \mathbb{Z}_p^*$ be an element of order q. Let $1 \leqslant a \leqslant q - 1$ and define $\beta = \alpha^a \mod p$. Furthermore, by G we denote the multiplicative subgroup of $\mathbb{Z}_p^*$ of order q. Note that G consists of the quadratic residues modulo p.

The values p, α and β are *public* and a is kept *secret* by A.

The plaintext messages x are assumed to be elements of G and so are the ciphers (as we shall see in a moment).

A signs the plaintext message x by computing

$$y = sig(x) = x^a \mod p$$

Then she sends (y, x) to B.

Verification Protocol

The verification (for $x, y \in G$) is done by executing the following steps:

Step 1: B chooses randomly $e_1, e_2 \in \mathbb{Z}_q^*$.

Step 2: B computes (the challenge) $c = y^{e_1}\beta^{e_2} \mod p$ and sends it to A.

Step 3: A computes the modular inverse a^{-1} of a modulo q and then $d = c^{a^{-1}} \mod p$ and sends it to B.

Step 4: B accepts y as a valid signature if and only if

$$d \equiv x^{e_1}\alpha^{e_2} \mod p\ .$$

end

Remarks

We explain the roles of p and q in this scheme.

The scheme lives in $\mathbb{Z}_p$ but we need to be able to perform computations in a multiplicative subgroup G of $\mathbb{Z}_p^*$ of prime order.
In particular, we need to be able to compute inverses modulo $|G|$. This is the reason why $|G|$ should be prime. It is convenient to take a prime p such that $p = 2q + 1$, where q is prime, i.e., q is a *Sophie Germain prime*. In this way, the subgroup is as large as possible. This is desirable, since plaintexts and ciphers are both elements of G.

Properties of the Verification Protocol I

Claim 1. B will accept a valid signature y.

Proof. In the following computations, all exponents are assumed to be reduced modulo p:

First, observe that

$$d \equiv c^{a^{-1}} \equiv y^{e_1 a^{-1}} \beta^{e_2 a^{-1}} \mod p .$$

Since $\beta \equiv \alpha^a \mod p$ we have

$$\beta^{a^{-1}} \equiv \alpha \mod p .$$

Similarly, $y = x^a \mod p$ implies that $y^{a^{-1}} \equiv x \mod p$. Hence,

$$d \equiv x^{e_1} \alpha^{e_2} \mod p$$

as desired. This proves Claim 1. ∎

Example 1

We take $p = 467$. Thus, $q = (467 - 1)/2 = 233$. Then 2 is a generator of $\mathbb{Z}_p^*$. We can conclude that $2^2 = 4$ is a generator of G, the quadratic residues modulo p. Thus, we take $\alpha = 4$. Let $a = 101$ be A's secret number. Then

$$\beta = 4^{101} \equiv 449 \mod 467 \, .$$

Example 1

We take $p = 467$. Thus, $q = (467 - 1)/2 = 233$. Then 2 is a generator of $\mathbb{Z}_p^*$. We can conclude that $2^2 = 4$ is a generator of G, the quadratic residues modulo p. Thus, we take $\alpha = 4$. Let $a = 101$ be A's secret number. Then

$$\beta = 4^{101} \equiv 449 \mod 467 \,.$$

A wishes to sign the message $x = 119$.
Thus she computes

$$y = 119^{101} \equiv 129 \mod 467 \,.$$

Example 2 (continued)

Next, suppose B wants to verify the signature 129. Suppose, B has chosen at random $e_1 = 38$ and $e_2 = 397$. Then B computes

$$c = 129^{38} \cdot 449^{397} \equiv 13 \mod 467 \, .$$

A in turn first computes the modular inverse a^{-1} of 101 modulo 233 which is 30. Then she calculates

$$d = c^{a^{-1}} \mod 467 \equiv 13^{30} \equiv 9 \mod 467 \, .$$

Finally, B checks the response by verifying that

$$119^{38} \cdot 4^{397} \equiv 9 \mod 467 \, .$$

Hence, B accepts A's signature as valid.

Properties of the Verification Protocol II

Next, we prove that A cannot fool B into accepting a fraudulent signature as valid, except with a very small probability.

Properties of the Verification Protocol II

Next, we prove that A cannot fool B into accepting a fraudulent signature as valid, except with a very small probability.

Theorem 1

If $y \not\equiv x^a \mod p$, *then* B *will accept* y *as a valid signature for* x *with probability* $1/q$.

Properties of the Verification Protocol II

Next, we prove that A cannot fool B into accepting a fraudulent signature as valid, except with a very small probability.

Theorem 1

If $y \not\equiv x^a \mod p$, *then* B *will accept* y *as a valid signature for* x *with probability* $1/q$.

Proof. First we observe that each possible challenge c corresponds to exactly q ordered pairs (e_1, e_2). This is because y and β are both elements of the multiplicative group G of prime order q.

Properties of the Verification Protocol II

Next, we prove that A cannot fool B into accepting a fraudulent signature as valid, except with a very small probability.

Theorem 1

If $y \not\equiv x^a \mod p$, *then* B *will accept* y *as a valid signature for* x *with probability* $1/q$.

Proof. First we observe that each possible challenge c corresponds to exactly q ordered pairs (e_1, e_2). This is because y and β are both elements of the multiplicative group G of prime order q. Now, when A receives the challenge c she has no way of knowing which of the q possible pairs (e_1, e_2) B has been used to construct c.

Properties of the Verification Protocol III

Claim 2. If $y \not\equiv x^a \mod p$, then any possible response $d \in G$ that A might make is consistent with exactly one of the q possible ordered pairs (e_1, e_2).

Properties of the Verification Protocol III

Claim 2. If $y \not\equiv x^a \mod p$, then any possible response $d \in G$ that A might make is consistent with exactly one of the q possible ordered pairs (e_1, e_2).

Proof. Since α generates G, we can write any element g of G as a power of α, say $g = \alpha^z$ where the exponent z is determined uniquely modulo q. So, we can write

$$c = \alpha^i \quad d = \alpha^j \quad x = \alpha^k \quad \text{and} \quad y = \alpha^\ell ,$$

where $i, j, k, \ell \in \mathbb{Z}_q$ and all arithmetic is done modulo q. Consider the following two congruences:

$$\begin{aligned} c &\equiv y^{e_1}\beta^{e_2} \mod p \\ d &\equiv x^{e_1}\alpha^{e_2} \mod p \end{aligned}$$

Properties of the Verification Protocol IV

The system above is equivalent to the following system:

$$\begin{aligned} i &\equiv \ell e_1 + a e_2 \mod q \\ j &\equiv k e_1 + e_2 \mod q\,. \end{aligned}$$

Now, we are assuming that

$$y \not\equiv x^a \mod p\,,$$

so it follows that

$$\ell \not\equiv ak \mod q\,.$$

Hence, the coefficient matrix of this system of congruences modulo q has non-zero determinant. Therefore, there is a unique solution to the system. That is, every $d \in G$ is the correct response for exactly one of the q possible ordered pairs (e_1, e_2).

Properties of the Verification Protocol IV

Consequently, the probability that A gives B a response d that will be verified is is exactly $1/q$, and the theorem is shown. $\blacksquare$

Properties of the Verification Protocol IV

Consequently, the probability that A gives B a response d that will be verified is is exactly $1/q$, and the theorem is shown. $\blacksquare$

Finally, we turn our attention to the disavowal protocol. This protocol consists of two runs of the verification protocol.

The Disavowal Protocol

Step 1: B chooses $e_1, e_2 \in \mathbb{Z}_q^*$ at random.

Step 2: B computes $c = y^{e_1}\beta^{e_2} \mod p$ and sends it to A.

Step 3: A computes a^{-1} modulo q and then $d = c^{a^{-1}} \mod p$ and sends it to B.

Step 4: B verifies that $d \not\equiv x^{e_1}\alpha^{e_2} \mod p$.

Step 5: B chooses $f_1, f_2 \in \mathbb{Z}_q^*$ at random.

Step 6: B computes $C = y^{f_1}\beta^{f_2} \mod p$ and sends it to A.

Step 7: A computes a^{-1} modulo q and then $D = C^{a^{-1}} \mod p$ and sends it to B.

Step 8: B verifies that $D \not\equiv x^{f_1}\alpha^{f_2} \mod p$.

Step 9: B concludes that y is a forgery if and only if

$$\left(d\alpha^{-e_2}\right)^{f_1} \equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p\ .$$

Example 3

Again, we take $p = 467$, $q = 233$, $\alpha = 4$, $a = 101$ and $\beta = 449$.
Let message $x = 286$ be signed with the bogus signature $y = 83$.
A wants to convince B that the signature is *invalid*.
Furthermore, suppose B begins choosing at random values $e_1 = 45$ and $e_2 = 237$. B then computes

$$c = y^{e_1}\beta^{e_2} \equiv 83^{45}449^{237} \equiv 305 \mod 467 ,$$

and A responds with

$$d = c^{a^{-1}} \equiv 305^{30} \equiv 109 \mod 467 .$$

Then B computes $286^{45}4^{237} \equiv 149 \mod 467$.
Since $149 \neq 109$, B proceeds to Step 5 of the protocol.

Example 4 (continued)

Now, B chooses at random $f_1 = 125$ and $f_2 = 9$, and computes

$$C = 83^{125} 449^9 \equiv 270 \mod 467\,,$$

and A responds with

$$D = C^{a^{-1}} \equiv 270^{30} \equiv 68 \mod 467\,.$$

Now B verifies that $68 \not\equiv 286^{125} 4^9 \equiv 25 \mod 467$.
Thus, B performs the consistency check in Step 9 and obtains

$$\left(109 \cdot 4^{-237}\right)^{125} \equiv 188 \equiv \left(68 \cdot 4^{-9}\right)^{45} \mod 467\,.$$

Thus, the consistency check succeeds and B is convinced that the signature is *not* valid.

Remarks

Steps 1 through 4 and Steps 5 through 8 comprise two unsuccessful runs of the verification protocol. Step 9 is a "consistency check" that enables B to determine if A is forming her responses in the manner specified in the protocol.

Remarks

Steps 1 through 4 and Steps 5 through 8 comprise two unsuccessful runs of the verification protocol. Step 9 is a "consistency check" that enables B to determine if A is forming her responses in the manner specified in the protocol.

We have to show two things at this point.

(1) A can convince B that an invalid signature is a forgery.

(2) A cannot make B believe that a valid signature is a forgery except with a very small probability.

Remarks

Steps 1 through 4 and Steps 5 through 8 comprise two unsuccessful runs of the verification protocol. Step 9 is a “consistency check” that enables B to determine if A is forming her responses in the manner specified in the protocol.

We have to show two things at this point.

(1) A can convince B that an invalid signature is a forgery.

(2) A cannot make B believe that a valid signature is a forgery except with a very small probability.

First, we show the following:

Properties of the Disavowal Protocol I

Theorem 2

If $y \not\equiv x^a \mod p$, and B and A follow the disavowal protocol, then

$$\left(d\alpha^{-e_2}\right)^{f_1} \equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p \,.$$

Properties of the Disavowal Protocol I

Theorem 2

If $y \not\equiv x^a \mod p$, *and* B *and* A *follow the disavowal protocol, then*

$$\left(d\alpha^{-e_2}\right)^{f_1} \equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p\,.$$

Proof. Using the facts that

$$\begin{aligned} d &\equiv c^{a^{-1}} \mod p \\ c &\equiv y^{e_1}\beta^{e_2} \mod p \quad \text{and} \\ \beta &\equiv \alpha^a \mod p\,, \quad \text{we have that} \end{aligned}$$

$$\begin{aligned} \left(d\alpha^{-e_2}\right)^{f_1} &\equiv \left(\left(y^{e_1}\beta^{e_2}\right)^{a^{-1}}\alpha^{-e_2}\right)^{f_1} \mod p \\ &\equiv y^{e_1 f_1}\beta^{e_2 a^{-1} f_1}\alpha^{-e_2 f_1} \mod p \\ &\equiv y^{e_1 f_1}\alpha^{e_2 f_1}\alpha^{-e_2 f_1} \mod p \\ &\equiv y^{e_1 f_1} \mod p\,. \end{aligned}$$

Properties of the Disavowal Protocol II

Using the facts that

$$
\begin{aligned}
D &\equiv C^{a^{-1}} \mod p \\
C &\equiv y^{f_1}\beta^{f_2} \mod p \ \text{ and} \\
\beta &\equiv \alpha^{a} \mod p ,
\end{aligned}
$$

a similar computation establishes that

$$\left(D\alpha^{-f_2}\right)^{e_1} \equiv y^{e_1 f_1} \mod p ,$$

and therefore the consistency check in Step 9 succeeds. $\blacksquare$

Properties of the Disavowal Protocol III

Now we look at the possibility that A might attempt to disavow a valid signature.
In this situation we do *not* assume that A follows the protocol.
That is, A might not construct d and D as specified by the protocol.

Hence, in the following theorem, we only assume that A is able to produce values d and D which satisfy the conditions in Steps 4, 8, and 9 of the *Disavowal Protocol* presented above.

Properties of the Disavowal Protocol IV

Theorem 3

Suppose $y \equiv x^a \mod p$ *and* B *follows the* Disavowal Protocol. *If*

$$d \not\equiv x^{e_1}\alpha^{e_2} \mod p$$

and

$$D \not\equiv x^{f_1}\alpha^{f_2} \mod p$$

then the probability that

$$\left(d\alpha^{-e_2}\right)^{f_1} \not\equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p$$

is $1 - 1/q$.

Proof. The proof is done indirectly.

Properties of the Disavowal Protocol V

Suppose the following is satisfied:

$$\begin{aligned} y &\equiv x^{a} \mod p \\ d &\not\equiv x^{e_1}\alpha^{e_2} \mod p \\ D &\not\equiv x^{f_1}\alpha^{f_2} \mod p \\ \left(d\alpha^{-e_2}\right)^{f_1} &\equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p\,. \end{aligned}$$

We shall derive a contradiction as follows:
The consistency check (cf. Step 9) can be rewritten in the following form:

$$D \equiv d_0^{f_1}\alpha^{f_2} \mod p\,,$$

where

$$d_0 = d^{1/e_1}\alpha^{-e_2/e_1} \mod p$$

is a value that depends only on steps 1 through 4 of the *Disavowal protocol*.

Properties of the Disavowal Protocol V

Suppose the following is satisfied:

$$\begin{aligned} y &\equiv x^{a} \mod p \\ d &\not\equiv x^{e_1}\alpha^{e_2} \mod p \\ D &\not\equiv x^{f_1}\alpha^{f_2} \mod p \\ \left(d\alpha^{-e_2}\right)^{f_1} &\equiv \left(D\alpha^{-f_2}\right)^{e_1} \mod p\,. \end{aligned}$$

We shall derive a contradiction as follows:
The consistency check (cf. Step 9) can be rewritten in the following form:

$$D \equiv d_0^{f_1}\alpha^{f_2} \mod p\,,$$

where

$$d_0 = d^{1/e_1}\alpha^{-e_2/e_1} \mod p$$

is a value that depends only on steps 1 through 4 of the *Disavowal protocol*.

Properties of the Disavowal Protocol VI

Applying Theorem 1, we conclude that y is a valid signature for d_0 with probability $1 - 1/q$. But we are assuming that y is a valid signature for x. That is, with high probability we have

$$x^a \equiv d_0^a \mod p$$

which implies that $x = d_0$.

Properties of the Disavowal Protocol VI

Applying Theorem 1, we conclude that y is a valid signature for d_0 with probability $1 - 1/q$. But we are assuming that y is a valid signature for x. That is, with high probability we have

$$x^a \equiv d_0^a \mod p$$

which implies that $x = d_0$.

However, the fact that

$$d \not\equiv x^{e_1}\alpha^{e_2} \mod p$$

means that that

$$x \not\equiv d^{1/e_1}\alpha^{-e_2/e_1} \mod p \, .$$

Properties of the Disavowal Protocol VII

Since

$$d_0 \equiv d^{1/e_1}\alpha^{-e_2/e_1} \mod p$$

we conclude that $x \neq d_0$, and we have a contradiction. $\blacksquare$

Thank you!