Signatures

CS/ECE 598MAN: Applied Cryptography

Nikita Borisov

December 4, 2009

Digital Signature Properties

Signature Properties

- Authentication
- Third-party verifiability
- Non-repudiation

Digital Signature Properties

Signature Properties

- Authentication
- Third-party verifiability
- Non-repudiation

But what if we don't want all of these properties?

Crypto Real Estate

Alice Bank

Bob

I'd like a mortgage

Crypto Real Estate

Alice Bank	Bob
	I'd like a mortgage
You're pre-approved for $100,000	

Crypto Real Estate

Alice Bank	Bob
	I'd like a mortgage
You're pre-approved for $100,000	Can I get that in writing?

Crypto Real Estate

Alice Bank	Bob
	I'd like a mortgage Can I get that in writing?
You're pre-approved for $100,000	
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")	

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		
	Charlie, can you do better?	

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")	Charlie, can you do better?	$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")
	Charlie, can you do better?	
	Alice, can you beat that?	

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")
	Charlie, can you do better?	
$\mathrm{Sign}_{\mathrm{Alice}}$("... $100,002")	Alice, can you beat that?	

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")
	Charlie, can you do better?	
$\mathrm{Sign}_{\mathrm{Alice}}$("... $100,002")		
	Alice, can you beat that?	
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $1,000,000")		
	...	

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")
	Charlie, can you do better?	
$\mathrm{Sign}_{\mathrm{Alice}}$("... $100,002")	Alice, can you beat that?	
	...	
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $1,000,000")		

How can Bob and Charlie prevent this?

Crypto Real Estate

Alice Bank	Bob	Charlie Financial
	I'd like a mortgage Can I get that in writing?	
You're pre-approved for $100,000		
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $100,000")		$\mathrm{Sign}_{\mathrm{Charlie}}$("Bob is pre-approved $100,001")
	Charlie, can you do better?	
$\mathrm{Sign}_{\mathrm{Alice}}$("... $100,002")	Alice, can you beat that?	
	...	
$\mathrm{Sign}_{\mathrm{Alice}}$("Bob is pre-approved for $1,000,000")		

How can Bob and Charlie prevent this?

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Alice Bank	David's Realty	Charlie Financial
	Is Bob pre-approved for a mortgage?	

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Alice Bank	David's Realty	Charlie Financial
	Is Bob pre-approved for a mortgage?	
Yes, $100,000		

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Alice Bank	David's Realty	Charlie Financial
	Is Bob pre-approved for a mortgage?	
Yes, $100,000		
		Is Bob pre-approved for a mortgage?

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Alice Bank	David's Realty	Charlie Financial
	Is Bob pre-approved for a mortgage?	
Yes, $100,000		
		Is Bob pre-approved for a mortgage?
I'm not telling you!		

Crypto Real Estate

Alice sets up a verification website, run with SSL, that can be used only by realtors.

Alice Bank	David's Realty	Charlie Financial
	Is Bob pre-approved for a mortgage?	
Yes, $100,000		
		Is Bob pre-approved for a mortgage?
I'm not telling you!		

But on closing day, Alice changes her mind and disavows any promises to David or Bob!

Undeniable Signatures

Undeniable signatures:

- Can only be verified with help of signer
- Cannot later be disavowed

Other applications: resisting blackmail.

Construction

[Chaum,van Antwerpen, CRYPTO'89; Chaum, EUROCRYPT'90]

Setup

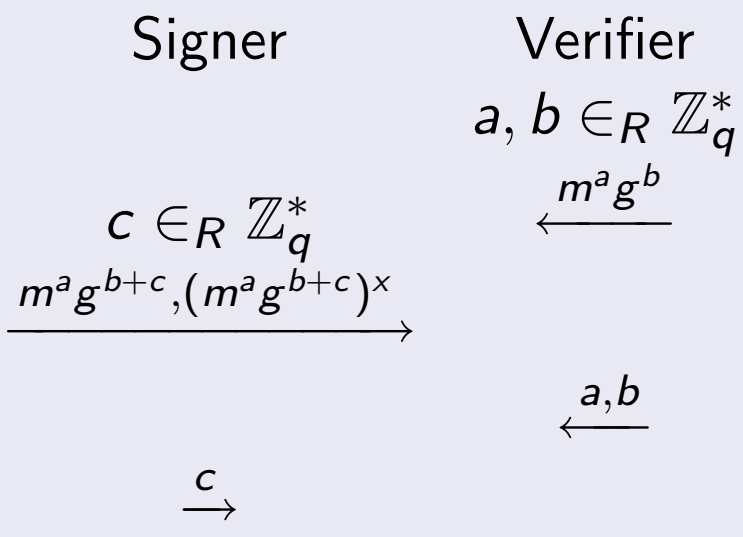
Generate private key $x \in \mathbb{Z}_q^*$, public key $y = g^x \bmod p$, where g is a generator of the group of order q in $\mathbb{Z}_p$.
A signature on a message m is $m^x \bmod p$

Construction

[Chaum,van Antwerpen, CRYPTO'89; Chaum, EUROCRYPT'90]

Verification

Verifier has z, wants to check whether $z = m^x \bmod p$



Note: $(m^a g^{b+c})^x = m^{ax} g^{(b+c)x} = z^a y^{b+c}$.

Construction

[Chaum,van Antwerpen, CRYPTO'89; Chaum, EUROCRYPT'90]

Disavowal

Signer proves that $z \neq m^x \bmod p$

Signer		Verifier
		$a \in_R \mathbb{Z}_q, s \in_R \mathbb{Z}_k$
	$\xleftarrow{m^s g^a, z^s g^{xa}}$	
$s' = (m^s g^a)^x / (z^s g^{xa})$		
$s = \log_{(m/z)^x} s'$		
$\xrightarrow{\text{Commit}(s,r)}$		
	$\xleftarrow{a}$	
$\xrightarrow{r}$		

Note: k must be small enough for a brute-force search. Can repeat protocol l times to get $1/(k+1)^l$ chance of cheating.

Man-in-the-middle Attack

Bob will want to verify Alice's protocol himself.
Bob can *relay* messages to Charlie, letting Charlie pick the random numbers. Alice think she's talking with Bob. (Adaptation of [Desmedt et al., CRYPTO'87])

Man-in-the-middle Attack

Bob will want to verify Alice's protocol himself.
Bob can *relay* messages to Charlie, letting Charlie pick the random numbers. Alice think she's talking with Bob. (Adaptation of [Desmedt et al., CRYPTO'87])
Extensions:

- Bob can mix in his own randomness, so that both are convinced
- n people can combine randomness to simultaneously verify a message through a single interaction with Alice ([Desmedt,Yung, EUROCRYPT'91])
- Alice does not know which message she is verifying ([Jakobsson, EUROCRYPT'94])

Man-in-the-middle Attack

Bob will want to verify Alice's protocol himself.
Bob can *relay* messages to Charlie, letting Charlie pick the random numbers. Alice think she's talking with Bob. (Adaptation of [Desmedt et al., CRYPTO'87])
Extensions:

- Bob can mix in his own randomness, so that both are convinced
- n people can combine randomness to simultaneously verify a message through a single interaction with Alice ([Desmedt,Yung, EUROCRYPT'91])
- Alice does not know which message she is verifying ([Jakobsson, EUROCRYPT'94])

Need to tie verification to verifier!

Designated Verifier Undeniable Signatures

Recall: verify protocol is a ZK-proof that $z = m^x$.

$$PK\{(\xi) : y_{\text{Alice}} = g^{\xi} \wedge z = m^{\xi}\}$$

A designated verifier proof adds another clause to the proof:

$$PK\{(\xi, \xi') : (y_{\text{Alice}} = g^{\xi} \wedge z = m^{\xi}) \vee (y_{\text{Bob}} = g^{\xi'})\}$$

Bob can always build such a proof, so he cannot convince anyone else.

Trap-door Commitments

A trap-door commitment is defined over a public/private key pair. Given only public key, the commitment scheme is secure, but it can be broken given the secret key.

Syntax

- $\text{Gen}(1^k)$: Generate (sk, pk)
- $\text{Commit}(pk, w, r)$: Generate a commitment c to w
- $\text{Trapdoor}(pk, sk, w, r, w')$: Generate r' such that $\text{Commit}(pk, w, r) = \text{Commit}(pk, w', r')$

Example

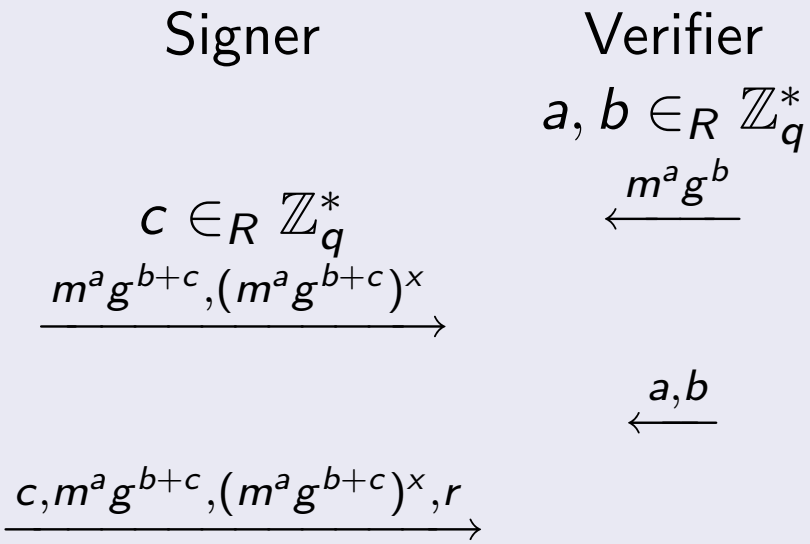
[Brassard,Chaum,Crépeau, JCSS'88]

- Gen(1^k): Generate an ElGamal public private keypair $(x, y = g^x \bmod p)$ (where g is the generator of the subgroup of order q in $\mathbb{Z}_p$).
- Commit$(y, w, r) = g^w y^r \bmod p$
- Trapdoor$(x, y, w, r, w') = (w - w')/x + r \bmod q$

$$g^{w'} y^{(w-w')/x+r} = g^{w'+(w-w')+xr} = g^w g^{xr} = g^w y^r \bmod p$$

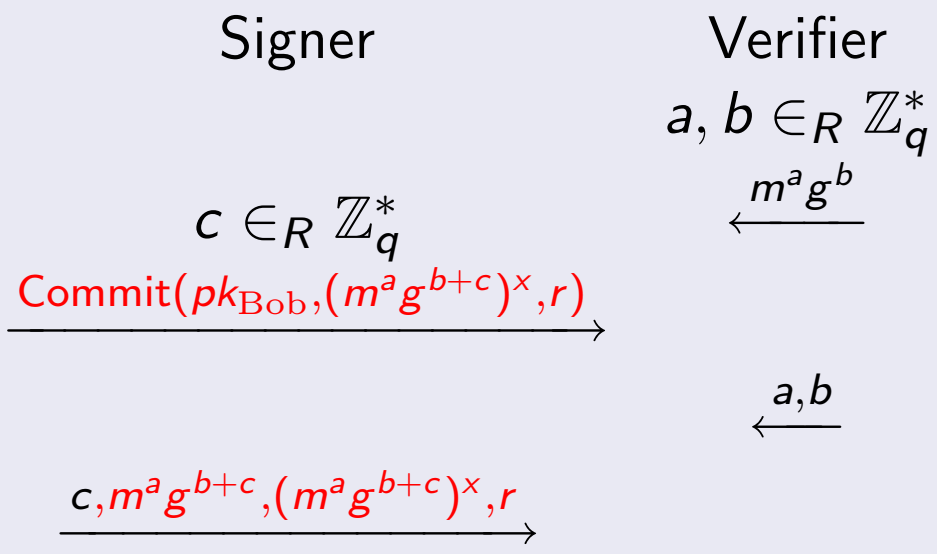
Designated Verifier Protocol
[Jakobsson et al.,EUROCRYPT'96]

Protocol



Designated Verifier Protocol
[Jakobsson et al.,EUROCRYPT'96]

Protocol



Alice uses a trapdoor commitment that Bob can break, and only opens it after seeing the challenges a, b.

Designated Verifier Non-interactive Proofs

Can use the same trick with non-interactive proofs.

- Three-move proof: (Commit,Challenge,Response) $= (c, a, r)$
- Fiat-Shamir: $a' = H(c)$
- Designated-Verifier: $a' = H(\mathrm{TD-Commit}(pk_{\mathrm{Bob}}, c, s))$, $r' = (r, s)$

Bob can break the commitment and generate new proof
Note: can be used to generated designated-verifier signatures

How to Leak a Secret
[Rivest et al., ASIACRYPT'01]

Problem

Cabinet member wants to leak a story to a journalist. But journalist's editor must verify the source of the leak, and cabinet member does not want the editor to know his name.

Cannot solve this with DV signatures (why not?)

How to Leak a Secret
[Rivest et al., ASIACRYPT'01]

Problem

Cabinet member wants to leak a story to a journalist. But journalist's editor must verify the source of the leak, and cabinet member does not want the editor to know his name.

Cannot solve this with DV signatures (why not?)

Ring Signatures

A ring signature on a message m shows that one of a set ("ring") of members has signed a message, but not which one.

Construction

Consider simple RSA:

RSA

$$\text{Sign}(m, n, d) = H(m)^d \bmod n$$

$$\text{Verify}(m, \sigma, n, e) : H(m) \stackrel{?}{=} \sigma^e \bmod n$$

Ring signature

Set of public keys (n_i, e_i) and private keys d_i for $i = 1, \ldots k$.
Assume wolog that the first person is actually signing.

1. Pick random values $\sigma_2, \ldots, \sigma_k \in \mathbb{Z}_n$
2. Compute $x_i = \sigma_i^{e_i} \bmod n_i$
3. Let $x_1 = H(m) \oplus x_2 \oplus \cdots x_k$
4. Compute $\sigma_1 = x_1^{d_1} \bmod n_1$
5. Signature: $(\sigma_1, \ldots, \sigma_n)$

Note

- A ring signature with ring $\{\mathrm{Alice}, \mathrm{Bob}\}$ is similar to a signature by Alice designated for Bob.
- Indeed, $\mathrm{Commit}(pk, c, r) = E_{pk}(c) \oplus E_{pk}(r)$ is a trapdoor commitment scheme.

Mesh Signatures
[Boyen, EUROCRYPT'07]

- Ring signatures prove that "Alice signed m" OR "Bob signed m" OR ...
- Mesh signatures extend this to more complicated clauses

Definition

Mesh Signatures

$$
\begin{aligned}
E ::= & [VK : M] \\
& | E_1 \vee E_2 \\
& | E_1 \wedge E_2 \\
& | \geq_t \{E_1, \ldots, E_m\} \qquad (t \text{ out of } m \text{ threshold})
\end{aligned}
$$

Mesh Signature Examples

- Ring signatures:

$$[VK_1 : M] \vee [VK_2 : M] \vee \ldots [VK_k : M]$$

- Messages can be different:

$$[VK_1 : M_1] \vee [VK_2 : M_2]$$

- Threshold

$$2\text{-out-of-}3\{[CEO : memo], [CFO : memo], [COO : memo]\}$$

- Certificate chains

$$[VK_1 : M_1] \vee ([VK_{CA} : VK_2] \wedge [VK_2 : M_2])$$

Group Signatures

- Ring signatures are linear in size
- Ring signatures provide absolute anonymity

Group Signatures

- Ring signatures are linear in size
- Ring signatures provide absolute anonymity

Definition

Ring Signatures

- $\text{Gen}(1^k) : (gpk, gmsk, gsk[i])$. $gmsk$ is master secret key, $gsk[i]$ is a secret key assigned to each member of group.
- $\text{Sign}(gpk, gsk[i], M)$: Produce a signature σ on M using one of the group keys
- $\text{Verify}(gpk, M, \sigma)$: Verify the signature, given a public key
- $\text{Open}(gpk, gsk, M, \sigma)$: Trace a signature to member i