Conditional Digital Signatures

Marek Klonowski, Mirosław Kutyłowski, Anna Lauks,
Filip Zagórski

Wrocław University of Technology

TrustBus 2005

Idea of Conditional Signatures

Conditional Digital Signature = a signature that is conditioned upon a certain event.

Examples:

- signature that is valid only if Bob has signed document M,
- signature that is valid after 20 September 2006.

Previous Solutions

- The contents of signed message had to be changed,
- the condition was expressed in a natural language.

Example:

To add a condition:

„This document is valid only if a document M_2 with hash value 168291bgb3vgVIQ719 has been signed by Bob.”

New Approach

- Scenario:
  - Alice's signature of M_1 is conditioned by Bob's signature of M_2.
- Steps of the protocol:
  - Bob publishes a commitment - a parameter related to the future signature of M_2,
  - Alice prepares a pre-signature of M_1,
  - Bob signs M_2,
  - using Bob's signature of M_2, signature of M_1 can be retrieved from the pre-signature.

Features of New Approach

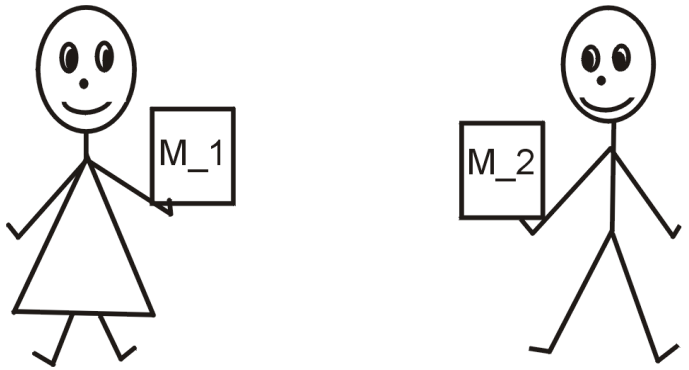
- There is no change of the message contents,
- until Bob signs M_2 it is infeasible to recover Alice's signature of M_1,
- Alice's signature retrieved from the pre-signature:
  - is a standard verifiable signature,
  - has no reference to M_2 or Bob.

ElGamal Based CDS - Assumptions

- Alice and Bob use the same group $\mathbb{Z}_p^*$,
- p - a prime number with hard discrete logarithm problem,
- g - generator of $\mathbb{Z}_p^*$,
- all operations modulo p.

ElGamal Based CDS - Assumptions

Alice wants to generate signature of M_1 conditioned by a Bob's signature of M_2.



	Alice	**Bob**
private key	$x_1 < p-1$	$x_2 < p-1$
public key	$y_1 = g^{x_1}$	$y_2 = g^{x_2}$

Creation of a Commitment

- k_2 - random number co - prime with $p-1$,
- $a_2 = g^{k_2}$,
- $S = g^{H(M_2)} y_2^{-a_2}$,
- (a_2, S) - commitment of Bob, published or given to Alice.

Key Property

If (a_2, b_2) is a valid ElGamal signature of M_2, then $S = a_2^{b_2}$.

Key Property

If (a_2, b_2) is a valid ElGamal signature of M_2, then $S = a_2^{b_2}$.

Indeed,

1. $S = g^{H(M_2)} y_2^{-a_2}$

Key Property

If (a_2, b_2) is a valid ElGamal signature of M_2, then $S = a_2^{b_2}$.

Indeed,

1. $S = g^{H(M_2)} y_2^{-a_2}$
2. ElGamal signature (a_2, b_2) is valid

$$\Longleftrightarrow \quad a_2^{b_2} \cdot y_2^{a_2} = g^{H(M_2)}$$

Creation of a PreSignature

- (a_2, S) - commitment of Bob,
- k_1 - a random number co - prime with $p-1$,
- (a_1, b_1) - a standard ElGamal signature of M_1,
  - $a_1 = g^{k_1}$,
  - $b_1 = k_1^{-1} \cdot (H(M_1) - x_1 a_1)$,
- z - random value,
- $(a_1, b_1 \cdot S^z, a_2^z)$ - presignature of M_1 conditioned by Bob's signature of M_2.

Signature Retrieval

- $(a_1, b_1 \cdot S^z, a_2^z)$ - Alice's presignature of M_1,
- (a_2, b_2) - Bob's signature of M_2 is published,
  - $b_2 = k_2^{-1} \cdot (H(M_2) - x_2 a_2)$,
  - $S = a_2^{b_2}$.

Retrieval of b_1 from the presignature:

$$\frac{b_1 S^z}{(a_2^z)^{b_2}} = \frac{b_1 S^z}{\left(a_2^{b_2}\right)^z} = \frac{b_1 S^z}{S^z} = b_1$$

Multiple Conditions

- Scenario:
  - We want messages $M_2, \ldots M_k$ to be signed before someone may derive a signature of M_1 from a presignature.
- Solution:
  - Multiple conditions scheme.

Multiple Conditions - Commitments

- commitments (a_i, S_i) for $i = 2, \ldots, k$
  - $a_i = g^{k_i}$ for a random k_i,
  - $S_i = g^{H(M_i)} y_i^{a_i}$, where y_i is the public key of the party that is supposed to sign M_i.

Multiple Conditions - PreSignature Creation

- (a_i, S_i) for $i = 2, \ldots k$ - commitments,
- k_1 - random number co-prime with $p - 1$,
- (a_1, b_1) - standard ElGamal signature of M_1,
- $z_2, \ldots z_k$ - random numbers.

Pre-Signature of M_1 conditioned by signatures of $M_2, \ldots, M_k$:

$$(a_1, b_1 \cdot \prod_{i=2}^{k} S_i^{z_i},\ a_2^{z_2},\ \ldots,\ a_k^{z_k})$$

Multiple Conditions - Signature Retrieval

- Pre-signature of M_1:

$$\left(a_1, b_1 \cdot \prod_{i=2}^{k} S_i^{z_i}, a_2^{z_2}, \ldots, a_k^{z_k}\right)$$

- retrieval of b_1 is possible, if signatures (a_i, b_i) for $i = 2, \ldots k$ are published,
- retrieval based on equalities $S_i = a_i^{b_i}$.

CDS based on Undeniable Signatures

- Scenario:
  - Alice produces a pre-signature of M_1 using Bob commitment related to signature of M_2.

CDS based on Undeniable Signatures

- Scenario:
  - Alice produces a pre-signature of M_1 using Bob commitment related to signature of M_2.
- Problem:
  - How a third party can check that a pre-signature can be transformed into Alice's signature of M_1 after Bob signs M_2?

CDS based on Undeniable Signatures

- Scenario:
  - Alice produces a pre-signature of M_1 using Bob commitment related to signature of M_2.
- Problem:
  - How a third party can check that a pre-signature can be transformed into Alice's signature of M_1 after Bob signs M_2?
- Solution:
  - Conditional signatures based on undeniable signatures.

Applications

Digital Business

- Signing conditioned documents,
- fair stock exchange,
- secure credit cards and online transactions,
- ...

Applications

Time Authority

- an institution that periodically confirms the current time,
- example: on day X after hour Y Time Authority signs a message: *„today is X, the current time has passed Y”*,
- useful if we wish that signature of M_1 can be retrieved at a given future date.

Conclusions and Open Problems

- Construction of conditional signatures is relatively straightforward,
- finally we obtain standard signatures - ElGamal, undeniable.

Conclusions and Open Problems

Problem: The person signing the conditioning document has to prepare and publish a commitment long before signing the document.

How to construct a scheme that does not need any additional parameters?
Is it possible??

Thank you for attention!