A Non-Repudiable Bitstring Commitment Scheme Based on a Public-Key Cryptosystem

Jordi Castellà-Roca and Josep Domingo-Ferrer
Universitat Rovira i Virgili
Dept. of Computer Engineering and Mathematics
Av. Països Catalans 26, E-43007 Tarragona, Catalonia
E-mail {jcaste, jdomingo}@etse.urv.es

Abstract

Commitment schemes are building blocks for guaranteeing fairness in higher-level cryptographic protocols such as mental poker protocols and others. A party Alice commits to a value v (a bit or a bitstring) without revealing it. Alice should not be able to cheat by opening the commitment as $v' \neq v$ nor to deny having committed at all. Most commitment schemes in the literature rely on hash functions, which should be strongly collision-free for the scheme to be secure. Yet collision-freeness can only be empirically checked and cannot be met with total certainty. We present a commitment scheme which avoids hash functions by using a public-key cryptosystem instead.

Keywords: *Bit commitment, Mental poker.*

1. Introduction

Cryptographic protocols try to handle situations where there is mutual distrust between parties (*e.g.* e-gambling, e-contracts, etc.). It is essential in such protocols to be able to ensure that any incorrect behavior by one or several parties will be detected: for example, in mental poker, misbehavior detection is essential. Commitment schemes, introduced in [Blum82], are protocols very useful as building blocks to guarantee fairness in higher-level cryptographic protocols.

A commitment protocol consists of two distinct stages:

Commitment A party Alice publicly commits to a value v without revealing it (the published commitment does not disclose v).

Opening Alice can later open the commitment and show v. Furthermore, Alice cannot open the commitment to show a value different from v.

In addition to its inherent security properties described above, a commitment should be *non-repudiable*: it should not be possible for Alice to deny having committed to v. Non-repudiability can be achieved by having the commitment signed by the committing party.

The seminal proposal [Blum82] was limited to imitating coin flipping between two parties: one party commits to a bit value, then the second party makes a binary choice and the first party opens her commitment. In [Naor90], a general framework was introduced for building bit commitments using one-way functions. The drawback of those early schemes is that they only allow commitment to a single bit, whereas committing to a bitstring is a fundamental need in many cryptographic applications. Bitstring commitment schemes were presented in [Damg94] and [Hale96]. See [Schn96] for an overview on the state of the art in commitment schemes. Most commitment schemes in the literature are based on hash functions, which causes them to share two shortcomings:

1. The hash functions used should be strongly collision-free. However, this property can only be empirically checked. It actually turns out that some schemes are inadvertently based on weakly collision-free hash functions ([Pren99]).

2. Hash functions alone cannot offer non-repudiability.

1.1. Our contribution

We present in this paper a bitstring commitment scheme which guarantees protection against cheating and repudiation by using a public-key cryptosystem rather than a hash function.

Section 2 describes the proposed commitment scheme. Section 3 contains a security analysis. Section 4 is a conclusion.

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)
0-7695-2108-8/04 $ 20.00 © 2004 IEEE

IEEE COMPUTER SOCIETY

2. The scheme

The scheme consists of two protocols: a commitment protocol and a protocol for opening/verifying the commitment.

Protocol 1 (Non-repudiable bitstring commitment)

1. Initial state: *The committing party Alice is assumed to have an asymmetric key pair (P_A, S_A), where P_A is the public key and S_A is the private key. Further, it is assumed that P_A is duly certified and publicly accessible.*
2. *Alice chooses the bitstring v to which she wishes to commit.*
3. *Alice generates a secret pseudo-random value r.*
4. *Alice concatenates her identifier Id_A with v to obtain $V := Id_A||v$.*
5. *Alice concatenates her identifier Id_A with r to obtain $R := Id_A||r$.*
6. *Alice signs V to obtain $S_A(V)$ and encrypts R under P_A to obtain $P_A(R)$.*
7. *The commitment C_A to be published is obtained as*

$$C_A := S_A(V) \oplus P_A(R) \tag{1}$$

   where $\oplus$ denotes modulo 2 bitwise addition.

8. *Alice publishes C_A.*

Alice can open the commitment C_A and any party Bob can verify it as described next:

Protocol 2 (Commitment opening and verification)

1. *Alice reveals the value r to a verifier Bob (in fact, Alice can publish r at large).*
2. *The verifier Bob encrypts $Id_A||r$ under P_A to obtain $P_A(Id_A||r)$ and retrieves $S_A(V)$ as*

$$C_A \oplus P_A(Id_A||r) = S_A(V) \tag{2}$$

3. *Bob encrypts $S_A(V)$ under P_A to obtain V.*
4. *Bob verifies that V contains Id_A as prefix (if everything is correct, one should have $V = Id_A||v$).*
5. *The commitment is deemed valid if and only if Id_A is a prefix of V. In that case, the suffix v of V is taken as the value committed to.*

3. Security analysis

Let us now analyze the security of the proposed commitment scheme.

Theorem 1 *If a sound public-key cryptosystem and a sound pseudo-random number generator are used, the commitment scheme specified by Protocols 1 and 2 satisfies that: i) C_A does not reveal v; ii) the probability of the committing party Alice being able to open C_A as $v' \neq v$ is $2^{-|Id_A|}$, where $|Id_A|$ is the bitlength of Id_A; iii) the committing party Alice cannot repudiate C_A.*

Proof: Let us first check the property that C_A does not reveal v. From Expression (1), C_A can actually be viewed as the result of encrypting $S_A(V)$ using a stream cipher with pseudo-random key $P_A(R)$; thus, the secrecy of $S_A(V)$ (and thus of v) depends on the r in $R = Id_A||r$ being generated using a cryptographically sound pseudo-random number generator (like those used in good stream ciphers).

Let us now derive the probability that the commitment can be non-uniquely opened. For Alice to open C_A as $v' \neq v$, one must have $C_A \oplus P_A(Id_A||r') = S_A(Id_A||v')$ for some value r'. This is equivalent to requiring that $Id_A||r' = S_A(C_A \oplus S_A(Id_A||v'))$ for some value r'. If a sound public-key cryptosystem is used, the probability that the prefix of $S_A(C_A \oplus S_A(Id_A||v'))$ matches Id_A can be approximated by $2^{-|Id_A|}$ where $|Id_A|$ is the bitlength of Id_A.

Finally, non-repudiability of C_A follows from the fact that the value v committed to is concatenated to Alice's identifier Id_A and the whole is signed by Alice as $S_A(Id_A||v)$. □

Note that, if $|Id_A| \geq 32$, the probability of non-uniquely opening the commitment given by Theorem 1 is already negligible. An application of the commitment scheme described here to implement fairness in e-gambling is described in Patent [Cast02].

4. Conclusion

Non-repudiable commitment schemes are an essential part of secure e-gaming and e-gambling protocols. In fact, such schemes are a guarantee that player misbehaviors or deviations from the protocols will be detected.

Using a public-key cryptosystem to construct a commitment is a way of achieving non-repudiability, a property which cannot be offered by hash functions alone. In this paper, we have presented a commitment scheme that allows a player to commit to a bitstring in a non-repudiable way. Obtaining the same properties with other schemes in the literature would require an additional digital signature on the commitment, which is avoided in our proposal.

IEEE COMPUTER SOCIETY

Acknowledgments

Thanks go to Jordi Herrera for useful suggestions and motivations. This work was partly supported by the Spanish Ministry of Science and Technology and the European FEDER Fund through project no. TIC-2001-0633-C03-01 "STREAMOBILE".

References

[Blum82] M. Blum, "Coin flipping by telephone: a protocol for solving impossible problems", *Proc. IEEE Computer Conference*, pp. 133-137, 1982.

[Cast02] J. Castellà-Roca, A. Riera-Jorba, J. Borrell-Viader and J. Domingo-Ferrer, "A method for obtaining an impartial result in a game over a communications network and related protocols and programs", international patent PCT ES02/00485, Oct. 14, 2002.

[Damg94] I. B. Damgaard, T. P. Pedersen and B. Pfitzmann, "On the existence of statistically hiding bit commitment schemes and fail-stop signatures", in *Advances in Cryptology-Crypto'93*, LNCS 773, Berlin: Springer, pp. 250-265, 1994.

[Hale96] S. Halevi and S. Micali, "Practical and provably secure commitment schemes from collision-free hashing", in *Advances in Cryptology-Crypto'96*, LNCS 1109, Berlin: Springer, pp. 201-215, 1996.

[Naor90] M. Naor, "Bit commitment using pseudo-randomness", in *Advances in Cryptology-Crypto'89*, LNCS 435, Berlin: Springer, pp. 128-136, 1990.

[Pren99] B. Preneel, "The state of cryptographic hash functions", in *Lectures on Data Security: Modern Cryptology in Theory and Practice*, LNCS 1561, Berlin: Springer, pp. 158-192, 1999.

[Schn96] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd Edition*, New York: Wiley, 1996.

IEEE COMPUTER SOCIETY