All-or Nothing Disclosure of Secrets

Gilles BRASSARD † and *Claude CREPEAU* ‡

Département d'informatique et de R.O.
Université de Montréal
Montréal (Québec)
Canada H3C 3J7

Jean-Marc ROBERT *

Département de Génie Electrique
Ecole Polytechnique de Montréal
Montréal (Québec)
Canada H3C 3A7

1. INTRODUCTION

Alice disposes of some number of secrets. She is willing to disclose one of them to Bob. Although she agrees to let him choose wich secret he wants, she is not willing to allow him to gain any information on more than one secret. On the other hand, Bob does not want Alice to know which secret he wishes. This is a useful building block in crypto-protocols. For instance, it can be used to easily implement a multi-party mental Poker protocol similar to that of [Cr1], i.e.: safe against player coalitions. An *all-or-nothing disclosure* is one by which, as soon as Bob has gained any information whatsoever on one of Alice's secrets, he has wasted his chances to learn anything about the other secrets. In particular, it must be impossible for Bob to gain joint information on several secrets, such as their exclusive-or. Notice that this is crucial, because it is well-known in classical cryptography that the exclusive-or of two plaintext English messages allows easy recovery of them both, just as a running stream Vigenère would [D].

We assume that Alice is honest when she claims to be willing to disclose one secret to Bob (i.e. she is not about to send junk). The only cheating Alice is susceptible of trying is to figure out which secret is of interest to Bob. Although equally worthwhile, we do *not* address here the problem of *verifiable* secrets [1], because it is too much application dependent. However, the problem of verifiable secrets is addressed and solved in [Cr2] for its specific application to mental poker.

Let us stress that the major novelty consists in letting Bob choose which secret he obtains. This is interesting whenever the secrets are not anonymous: although Bob does not know their contents, he knows their individual purpose [2]. Consider for instance the following situation: an international

† Supported in part by NSERC grant A4107.

‡ Supported in part by an NSERC postgraduate scholarship; current address: MIT.

* Current address: McGill University, Montréal.

1. That is, preventing that Bob unknowingly obtains a falsified secret should Alice fail to cooperate honestly.

2. In order to get a computationally secure scheme under cryptographic assumptions, it would otherwise suffice to use a variation on oblivious transfer (attributed to Oded Goldreich in [BPT]) to allow ''Alice to transfer to Bob exactly one out of two recognizable messages'' so that neither has control over which

spy disposes of a large corpus of various state secrets. He sells them by the piece to whoever is willing to pay the price. In his catalogue, each secret is advertised with a tantalizing title, such as ‘‘where is Abu Nidal’’. He would not accept to give away two secrets for the price of one, or even partial information on more than one secret. On the other hand, you (the potential buyer) would not pay for a randomly chosen secret, but are reluctant to let him know which secret you wish to acquire, because his knowledge of your specific interests could be a valuable secret for him to sell to someone else (under the title : ‘‘who is looking for terrorists’’, for instance). Let us point out that this problem was addressed and solved more that 15 years ago *by quantum physical means*, when the number of secrets is at most three, in Wiesner’s original Quantum Cryptography paper [W].

Under cryptographic assumptions, we provide in this paper a practical computationally secure solution. This solution is inspired by our work on zero-knowledge interactive protocols [BC1, BC2]. In a companion paper [BCR], we show how to efficiently reduce this general all-or-nothing disclosure of secrets problem to a much simpler problem known as the two-bit problem. The main interest of this reduction is that it is information theoretic and that it does not depend on unproved assumptions.

We assume that the reader has some number theoretic background, being familiar with the notation $\mathbb{Z}_m^*$, the notions of quadratic residues and Jacobi symbol, and the quadratic residuosity assumption (QRA) [GM]. We also assume the reader is familiar with the principle of zero-knowledge interactive proofs [GMR].

2. A SOLUTION BASED ON QUADRATIC RESIDUOSITY

Let $x_1, x_2, \ldots, x_n$ be Alice’s t-bit secrets, and let b_{ij} be x_i’s j^{th} bit for $1 \le i \le n$ and $1 \le j \le t$. Initially, Alice randomly selects two large distinct primes p and q together with a quadratic non-residue y modulo $m = pq$ whose Jacobi symbol is +1. For each secret bit b_{ij}, she selects a random $x_{ij} \in \mathbb{Z}_m^*$ and computes $z_{ij} = x_{ij}^2 y^{b_{ij}} \ \mathbf{mod}\ m$. Notice that z_{ij} is a quadratic residue if and only if $b_{ij} = 0$. Finally, Alice gives Bob both m and y, together with all the z_{ij}’s, keeping p and q secret. According to QRA, this does not enable Bob to obtain in polynomial time any information on Alice’s actual secrets.

If Bob wanted to know bit b_{ij} for some specific i and j, and if Alice were willing to cooperate, the following protocol comes to mind : Bob chooses a random $r \in \mathbb{Z}_m^*$ and a random bit a, he computes the question $q = z_{ij} r^2 y^a \ \mathbf{mod}\ m$ and he asks Alice for the quadratic residuosity of q. Clearly, $b_{ij} = a$ if and only if q is a quadratic residue. On the other hand, regardless of i and j, q is a completely random element of $\mathbb{Z}_m^*$ and thus Alice has no idea as to which of her secret bits she has just given away. One might naively be tempted to "solve" ANDOS by allowing Bob to ask t such questions, one for each bit of the secret he wants. There are three severe flaws with this idea :

- Bob could ask for t bits taken from distinct secrets.
- Bob could obtain in one question the exclusive-or of severals bits. For instance, he could ask the question $q = z_{ij} z_{kj} r^2 y^a \ \mathbf{mod}\ m$ and thus learn $b_{ij} \oplus b_{kj}$. As pointed out in the introduction, this would most probably enable him to obtain two complete secrets by asking for their exclusive-or, assuming the actual secrets are in plaintext English.

---

message will be received.

- More subtly, despite the previous claim, this would open the door for Alice to cheat as well! Indeed, she could lie from the beginning and give Bob a quadratic *residue* for her y. In this case, the questions asked by unsuspecting Bob would keep the same quadratic character as the corresponding z's, allowing Alice to figure out Bob's interests.

In order to solve these difficulties, it is imperative that both Alice and Bob convince the other of their good faith: Alice must show that the information she posted initially is genuine and Bob must convince Alice that his questions are honest. This is where zero-knowledge interactive protocols come into play. The third flaw mentioned above is solved by Alice using zero-knowledge interactive protocols of [GHY] and [GMR] to convince Bob that m has only two prime factors and that y is a quadratic *non*-residue modulo m, respectively. In a context of *verifiable* secret, this is also where Alice would convince Bob that the secrets hidden by the z_{ij}'s respect whichever conditions befit the application (a specific example is given in [Cr2]).

The first two flaws of the naive protocol above are harder to control. Although we have found several solutions, we only sketch here our favourite. Let σ be a permutation of $\{1, 2, \ldots, n\}$. A <u>σ-packet</u> P_σ consists of one question for each bit of each secret in the following way $P_\sigma = < q_{kj} \mid 1 \le k \le n, 1 \le j \le t >$ such that each $q_{kj} = z_{ij}\, r_{kj}^2\, y^{a_{kj}} \ \mathbf{mod}\ m$, where $i = \sigma^{-1}(k)$, r_{kj} is a random element of $\mathbb{Z}_m^*$ and a_{kj} is a random bit. Moreover, a σ-packet is <u>valid</u> if Bob knows the corresponding σ, r_{kj}'s and a_{kj}'s (notice that any collection of nt elements of $\mathbb{Z}_m^*$ with Jacobi symbol +1 is a σ-packet for every permutation σ, and Alice cannot distinguish a valid packet from any other such collection; however, assuming QRA, it is computationally infeasible for Bob to turn a random collection into a valid packet).

After the initialisation described previously, the ANDOS protocol proceeds as follows if x_i is the secret of interest to Bob.

- Bob randomly selects a permutation σ together with appropriate r_{kj}'s and a_{kj}'s, and forms a valid σ-packet P_σ.
- Bob gives P_σ to Alice, keeping secret his random information, and convinces her that it is a valid packet (see below).
- Bob sends $k = \sigma(i)$ to Alice as his actual request.
- Alice gives Bob the quadratic character of each q_{kj} in Bob's packet P_σ, for this specific k and each $1 \le j \le t$.
- Bob infers each of Alice's bits b_{ij} for $1 \le j \le t$, hence he obtains x_i as desired.
- If Bob wishes to obtain another secret and if Alice is willing to give (or sell) it to him, it suffices to repeat the three previous steps with the relevant new value for i; there is no need for Bob to form another packet and convince Alice of its validity all over again (unless it is important for the application that Alice does not even know if Bob's new request is for a different secret).

It is of course crucial that Alice be convinced that Bob's packet P_σ is valid, for he could otherwise stuff it with dishonest questions and we would be back to the beginning. It is equally crucial that Bob does not give Alice a clue as to which permutation σ he chose, for she might otherwise gain information on $\sigma^{-1}(k)$, the secret of interest to Bob. This is achieved by an idea very similar to those leading to the perfect zero-knowledge interactive protocol of [BC2]. Let s be a safety parameter agreed upon between Alice and Bob. After randomly choosing s additional permutations

$\sigma_1, \sigma_2, \ldots, \sigma_s$ of $\{1, 2, \ldots, n\}$, nts new elements of $\mathbb{Z}_m^*$ and nts new bits, Bob creates s additional σ_i-packets $P_1, P_2, \ldots, P_s$. He sends all these packets together with the original P_σ. At this point, Alice selects a random subset $X \subseteq \{1, 2, \ldots, s\}$ and sends it to Bob as a challenge. In order to convince her of the validity of P_σ, Bob must:

- for each $l \in X$, prove the validity of P_l to Alice by disclosing σ_l and all the random elements of $\mathbb{Z}_m^*$ and random bits used in the creation of P_l;
- for each $l \notin X$, prove to Alice that P_σ is valid if and only if P_l is valid by disclosing $\sigma_l^{-1}\sigma$ and showing that he is capable of transforming the questions in P_σ into the corresponding questions in P_l (we leave the details of this to the reader).

At the end of this subprotocol, Alice will be convinced that P_σ is valid, with a 2^{-s} probability of beeing fooled by Bob. Indeed, the only way he could convince her of the validity of an invalid P_σ would be by producing valid packets for each $l \in X$ and invalid packets for each $l \notin X$. Since he must do so before being told X, the result follows from the fact that Alice has 2^s different choices for X.

3. OUTLINE OF THE REDUCTIONS OF [BCR]

In [BCR], we give information theoretic reductions among disclosure problems. More precisely, we show that it is exactly as hard to all-or-nothing disclose one t-bit secret among n than it is to disclose one bit among two. This result is obtained by a chain of reductions that allows the collapse of an apparent hierarchy of disclosure problems. Here is a list of problems that turn out to be information-theoretically equivalent, that is even if either or both party(ies) had unlimited computing power, regardless of unproved assumptions.

The *two-bit problem* (2BP): Alice disposes of two secret bits and she is willing to disclose one of them to Bob, at his choosing. Bob must not be allowed to learn more than one bit of information on Alice's bits, but Alice will not be upset if Bob succeeds in gaining any (deterministic) one-bit function of these two bits, such as their exclusive-or. If Bob plays fair and obtains the physical bit of his choice, Alice does not know which of her two bits she disclosed.

The *all-or-nothing two-bit problem* (AN2BP): Alice disposes of two secret bits and she is willing to disclose one of them to Bob, at his choosing. Nothing Bob can do will give him more than one of these physical bits: as soon as he obtains any information on one of them, he looses all hopes to gain any information on the other. Alice does not know which of her two bits she disclosed.

The *all-or-nothing n-bit problem* (ANNBP): this is identical to the previous problem, except that Alice owns n secret bits rather than 2. She wishes to all-or-nothing disclose one of them to Bob, at Bob's choosing.

The *all-or-nothing disclosure of secrets* (ANDOS): described previously.

ACKNOWLEDGEMENTS

We wish to thank Oded Goldreich, Silvio Micali, René Peralta, Joel Seiferas and Umesh Vazirani for their valuable comments. David Chaum has indepently suggested a similar protocol based on RSA rather than quadratic residuosity [Ch]. Isabelle Duchesnay has suggested the international spy application. Gilles Brassard also wishes to thank Manuel Blum for his inspiring talk at the MIT Endicott House conference in June 1985.

REFERENCES

[BPT] R. Berger, R. Peralta and T. Tedrick, ''A Provably Secure Oblivious Transfer Protocol'', *Proceedings of EUROCRYPT 84*, 1984, pp. 379-386.

[BC1] G. Brassard and C. Crépeau, ''Zero-Knowledge Simulation of Boolean Circuits'', these *Advances in Cryptology: Proceedings of CRYPTO 86*, A. Odlyzko, ed., Springer-Verlag, 1987.

[BC2] G. Brassard and C. Crépeau, ''Non Transitive Transfert of Confidence: A *Perfect* Zero-Knowledge Interactive Protocol for SAT and beyond'', *Proceedings of the 27th Annual IEEE Symposium on the Foundations of Computer Science*, 1986, pp. 188-195.

[BCR] G. Brassard, C. Crépeau and J.-M. Robert, ''Information Theoretic Reduction among Disclosure Problems'', *Proceedings of the 27th Annual IEEE Symposium on the Foundations of Computer Science*, 1986, pp. 168-173.

[Ch] D. Chaum, *Private communication*, may 1986.

[Cr1] C. Crépeau, ''A Secure Poker Protocol That Minimizes the Effect of Player Coalitions'', *Advances in Cryptology: Proceedings of CRYPTO 85*, H. C. Williams, ed., Lecture Notes in Computer Science 218, Springer-Verlag, 1986, pp. 73-86.

[Cr2] C. Crépeau, ''A Zero-Knowledge Poker Protocol that Achieves Confidentiality of the Players' Strategy, *or* How to Achieve an Electronic Poker Face'', these *Advances in Cryptology: Proceedings of CRYPTO 86*, A. Odlyzko, ed., Springer-Verlag, 1987.

[D] D. E. R. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, Massachussetts, 1982.

[GHY] Z. Galil, S. Haber and M. Yung, ''A private interactive test of a Boolean predicate and minimum-knowledge public-key cryptosystems'', *Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science*, 1985, pp. 360-371.

[GM] S. Goldwasser and S. Micali, ''Probabilistic Encryption'', *Journal of Computer and System Sciences*, **28**, 1984, pp. 270-299.

[GMR] S. Goldwasser, S. Micali and C. Rackoff, ''The knowledge complexity of interactive proof-systems'', *Proceedings of the 17th Annual ACM Symposium on the Theory of Computing*, 1985, pp. 291-304.