New Directions in Cryptography: Summary

Oliver Vecchini

22$^{\text{nd}}$ March 2019

Abstract

The following is a summary of the contents, context, and consequences of a seminal paper in theoretical computer science, namely '*New Directions in Cryptography*', written by B. W. Diffie and M. E. Hellman and published in 1976 [1]. It is submitted as part of the assessed coursework component of the COMP0007 *Directed Reading* module at UCL.

1 Background

Prior to the late 1970s, the task of secure communication over insecure channels between two parties would have been achieved by one of many crytographic schemes (common choices included the Lucifer and DES ciphers [2]). Regardless of choice, any scheme would invariably follow the same base protocol of *secret-key encryption*, whose security relied on a secret key being known to the two parties and those two *only*. During this period, the only way of achieving this would be generation of the key by one, and transmission of it to the other over a secure channel; the existence of a secure channel would seem to render the system redundant. In practice, the key could be transmitted over an impractical but secure channel, and used several times for secret-key encryption over an insecure channel, although this re-use undermines security (for instance with the *one-time pad*, the only cipher in common use capable of unbreakable theoretical security, but reliant on the key never being re-used [2]).

While the terminology of *public-key* cryptography was introduced by Diffie and Hellman's paper, many of the concepts it describes had been derived earlier by others. By 1975, R. C. Merkle had derived the notion of exchanging a key between two parties securely over an insecure channel, with cryptanalysis rendered ineffective not due to its theoretical impossibility but its computational infeasability, as well as providing an instance of one such scheme [3]; however, due to publication delays, his work was published *after* Diffie and Hellman's (interestingly, the first publication of Merkle's paper was edited by R. L. Rivest, one of the inventors of the RSA public-key cipher, whose publication paper itself cites Merkle's [4]). While theoretically significant, the scheme described in his paper (later coined *Merkle's Puzzles*) was unsuitable for practical use; cryptanalysis of the scheme, while an inconvenience for an attacker, was definitely tractable, while attempts at increasing security required increasing channel bandwidth to unusable levels.

Prior even to this, researchers at GCHQ had not only proven the existence of a scheme matching the description of public-key encryption, but had also derived the exact procedures of the schemes later known as Diffie-Hellman key exchange and the RSA cryptosystem, all realised in the 1970s prior to the publication of Diffie and Hellman's paper, but not declassified until 1997 [5].

2 Contents of the article

The authors begin by expressing the increasing importance of advancements in cryptography, given the expansion of contemporary computer networks. An outline of cryptographic convention until then is presented, outlining the operation of secret-key cryptography, and the problems of privacy (assuring a sender that only a particular party *receives* a message) and one-way authentication (assuring a recipient that only a particular party could have *sent* a message). Preference is expressed towards *block* ciphers over *stream* ciphers (operating over messages totally and piecemeal respectively), as minor changes in plaintext effect major changes in ciphertext (*error propogation*); this has benefits for authentication, preventing attackers from splicing previous valid ciphertext into their own 'valid' ciphertext.

The novel material concept of the paper is the notion of *public-key cryptography*, motivated by the fact that with contemporary networks growing so quickly, it would soon become impractical to establish a secure channel for every pair of communicating parties; it would be preferable to communicate exclusively over normal (but insecure) channels using public information to establish private communications. Two possible schemes satisfying this are shown, namely *public-key cryptosystems* (PKCs) and *public-key distribution systems* (PKDs) introduced under the context of message privacy (although PKCs are shown to relate to authentication as well). PKCs are defined formally as sets of pairs of algorithms E_k, D_k for variable (seed) key k, which each transform a message into another message such that

- E_k is the inverse of D_k,
- E_k, D_k are computationally feasible for any message,
- Deriving one of D_k, k from E_k is generally computationally infeasible, and
- Deriving both E_k, D_k from k is computationally feasible.

As a result, if a party generates E_k, D_k from some key k, E_k can be freely published to some publicly-available trusted repository over a secure channel (as a 'public key'), needing only to keep D_k secret (as a 'private key'). To send a private message, a sender can use the public key of the intended recipient to encrypt it, and send the ciphertext to the recipient over a normal (insecure) channel; only the recipient can decrypt it using their private key. This eliminates the requirement for a secure channel between sender and recipient! An example is provided wherein E_k, D_k are represented by multiplication of an n-bit message vector with square matrices A and B respectively, where A, B are inverse of eachother. Generating two such matrices from a random key k takes $O(n^2)$ steps, while deriving one from the other takes $O(n^3)$ steps (although the factor of difference between the two is not large enough to yield practically viable security). Another example is presented relying on security by obscurity of E_k's implementation, however this custom is heavily frowned upon in modern practice [6].

PKDs cover a somewhat simpler problem, but which remove the requirement of secure channels nonetheless. The task is for two parties to reach consensus over a key to be used for secret-key encryption without a secure channel; Merkle had described the concept before and even provided a solution, although insecure. Diffie and Hellman here present a new solution, based on the discrete logarithm problem, or specifically the difficulty of calculating the integer k such that for some $a, b \in \mathbb{F}_p$ and prime p, $a = b^k$. The procedure for each party is:

1. Agree with the other party on a prime p and some $\alpha \in \mathbb{F}_p$ over the insecure channel.
2. Generate a random integer $X_i \in \mathbb{F}_p$, which is kept private to the party.
3. Calculate $Y_i = \alpha^{X_i}$ and sends it to the other over the insecure channel.
4. Calculate the same key across both parties using $K = Y_j^{X_i}$ $(= \alpha^{X_i X_j})$ $(i \neq j)$.

To perform cryptanalysis an attacker needs to derive K from Y_i, Y_j; the best method for this involves taking a discrete logarithm (e.g. $K = Y_i^{log_\alpha Y_j}$). This takes much longer than discrete exponentiation; if the latter takes n steps, the former takes $O(e^{cn})$ steps (for constant $c \neq 0$), implying that cryptanalytic effort grows exponentially relative to normal use.

Formally defining this concept, the authors discuss *one-way functions*, defined by the property of *preimage resistance* (that is, for most given outputs y, it is computationally infeasible to find a value x that maps to y), while remaining computationally feasible to evaluate. These are useful for storage of authentication information, with an example given in the context of login systems with storing password hashes instead of as plaintext. For general eavesdropping, the authors note that with a PKC, if a party X encrypts a message with their own private key and publishes the result (a *signature*), other parties can decrypt the ciphertext with X's public key to get a valid message, showing that only X could have sent it; this scheme produces viable one-way authentication. Other solutions are presented using one-way functions, although all are shown to be impractical.

The authors now link several of the concepts presented thus far to eachother. Firstly, it is noted that if a block cipher B is secure against attackers attempting to derive the secret key from any pair of plaintext/ciphertext, then a high-quality one-way function f can be constructed from it such that the domain of f is the keys of B, and f applied to some k returns the ciphertext C generated by encrypting some random message P with k (trying to infer k from C is, by security of B, infeasible); properties of this link (and alternative constructions) are discussed (in particular the utility of one-way functions in reasoning about cryptosystems). For the next connection, the authors coin some definitions with relation to PKCs. A *trap-door (one-way) function* matches the definition of a one-way function except that, for a given y, it is easy to find some x that maps to y if certain *trap-door information* is known. It is thus clear to consider PKCs as (bijective) trap-door functions whose evaluation, and derivation of inverse with, and without trap-door information, reflect application of the public key, application of the private key, and cryptanalysis respectively (the private key *is* the trap-door information). This also illustrates how PKCs can never attain perfect theoretical security, as the private key is always uniquely derivable from the public key. PKCs can also be used as PKDs (by transmitting a chosen key), although the converse is not true; this highlights an interesting duality between these two schemes and their underlying primitives, in that PKCs are a subset of PKDs, while trap-door functions are a subset of one-way functions.

Finally, the authors discuss how to apply complexity theory to formally classify computational infeasibility. They note the attractive property of *NP-complete* problems of being at least as hard as the hardest of NP-hard problems (and are thus intractable unless $P = NP$). However, analysis of these primarily concerns worst-case situations, while cryptographic design favours analysis of average-case situations (i.e. security in all cases); NP-complete problems are not necessarily intractible in the average case. The authors express that a potential method of deriving a good one-way function (and thus, a PKC by further adaption into a trap-door function) would be to adapt some NP-complete problem such that no algorithm exists to solve the problem in polynomial time in the average case, and there exists some algorithm to solve the inverse problem in polynomial time for all input. The one-way function is then the solution of the inverse problem. An example is given using the NP-complete knapsack problem, and adapted to improve average-case intractability, with flaws acknowledged.

3 Legacy

The influence of the paper in the field of theoretical computer science has been immeasurable, forming the root of an entire discipline of cryptography. The subsequent search for suitable trap-door one-way functions with intractible inverses for PKCs bore fruit with the RSA cryptosystem a year later, whose security is derived from the difficulty of factorising the product of two prime numbers [4]. Another family of cryptographic schemes, elliptic curve cryptography ('ECC'), uses methods based on the example PKD given in the paper (since coined *Diffie-Hellman key exchange*, or 'DH'), with the advantage of smaller key size than RSA for the same security [7]. These three schemes underpin the bulk of modern public-key cryptography; they form one half of the TLS/SSL security protocol (the *de facto* standard for Web encryption, for instance in securing HTTPS). Also directly derived from DH and the discrete logarithm problem are the ElGamal cryptosystem and the Digital Signature Algorithm ('DSA') [8].

One unmentioned problem that would seem to be critical to PKCs is the issue of authenticating a public key claiming to correspond to some party. The two chief solutions addressing this are the (centralised) *public-key infrastructure* model, relying on *certificate authorities* to attest to key validity (as used by TLS), and the (decentralised) *web of trust* model, where authentic keys are acquired through networks of trusted parties (as used by PGP) [8].

As the paper recommends, several PKCs have been derived from NP-complete problems, including the Merkle-Hellman knapsack, McEliece, and NTRUEncrypt cryptosystems, with trap-door functions based on the knapsack, linear code decoding, and shortest vector problem of lattices respectively. While the first of these has been broken, the latter two are distinct for being resistant to attack by quantum computers, as all of the previously mentioned problems are tractable using these with Shor's algorithm [9]. Otherwise, the suggestion of deriving PKCs from NP-complete problems seems unpopular, as many successful schemes use problems that are not even NP-hard (such as factorisation in RSA, or the discrete logarithm problem of DH); many now consider NP-completeness irrelevant to public-key cryptography [10].

Separate to the notions of PKCs and PKDs, the paper also stimulated development of digital authentication schemes. Schemes developed since then include the Rabin and Merkle signature schemes, as well as DSA; however, these all either rely on trap-door functions or omit a proof of security. The first scheme not reliant on trap-door functions that was proven to be secure was published by M. Naor and M. M. Yung in 1989 [11].

References

[1] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[2] Hans Delfs and Helmut Knebl. In *Introduction to Cryptography*. Springer, 2007.

[3] Ralph C Merkle. Secure communications over insecure channels. *CACM*, 21:294–9, 1978.

[4] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 1978.

[5] James H Ellis et al. The story of non-secret encryption. *CESG Report*, 1987.

[6] Kerckhoff's principle. `en.citizendium.org/wiki/Kerckhoffs'_Principle/`.

[7] Julio Lopez and Ricardo Dahab. An overview of elliptic curve cryptography. 2000.

[8] Kristen Dorey. An internet-wide analysis of diffie-hellman key exchange and x. 509 certificates in tls. 2017.

[9] Ray A Perlner and David A Cooper. Quantum resistant public key cryptography: a survey. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*. ACM, 2009.

[10] Christos H Papadimitriou. Np-completeness: A retrospective. In *International Colloquium on Automata, Languages, and Programming*, pages 2–6. Springer, 1997.

[11] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the 21st annual ACM symposium on Theory of computing*.