Improved key-reconciliation method

Ludo Tolhuizen, Ronald Rietman, Oscar Garcia-Morchon
{ludo.tolhuizen,ronald.rietman,oscar.garcia-morchon}@philips.com

In [1], Peikert proposed efficient and practical lattice-based protocols for key transport, encryption and authenticated key exchange. One of the main technical innovations of [1] is a reconciliation technique that allows two parties who "approximately agree" on a secret value to reach *exact* agreement, a setting common to essentially all lattice-based encryption schemes. In [1], this reconciliation technique was described for reaching agreement on a single bit. Peikert's reconciliation technique has been extended in [2], allowing for agreement on more than one bit. In both cases, only one reconciliation bit is required to reach exact agreement. As symmetric keys typically require many bits, say 128 or more, the parties compute multiple secret values, and reach exact agreement on each of those values individually.

In this paper, we propose a reconciliation method that sends more than one reconciliation bit. In this way, the parties can agree on the same number of bits as with Peikert's method with less stringent conditions on "how approximate" the approximate agreement must be. Allowing for less stringent conditions on the approximate agreement improves security of the system. Alternatively, with virtually the same approximation requirements (i.e., with virtually the same security guarantees), an instance of our method allows the two parties to agree on one a secret value that is one bit longer than with the method from [2]. We numerically illustrate the advantages of our method with the impact to the recommended schemes in [2].

Technical description

We use the following notation. If x, v are integers, with $v \geq 2$, then $\langle x \rangle_v$ is the integer satisfying

$$0 \leq \langle x \rangle_v \leq v - 1 \text{ and } \langle x \rangle_v \equiv x \bmod v.$$

Moreover, for any real number y, we denote with $\lfloor y \rfloor$ the result of round y downwards to the closest integer.

We consider the situation that parties $\mathcal{A}$ and $\mathcal{B}$ have computed two numbers a and b. Because of the way that a and b are have been computed, they approximately agree. This approximate agreement is expressed in terms of system constants q, B and δ, known to $\mathcal{A}$ and $\mathcal{B}$, where δ and B are positive integers, and q is an integer multiple of $2^{B+\delta+1}$, as follows: a and b both are integers in the interval $[0, q)$ and satisfy

$$a \equiv b + e \pmod{q} \tag{1}$$

where

$$|e| \leq \frac{q}{2^{B+1}} - \frac{q}{2^{B+\delta+1}}. \tag{2}$$

We will describe how the two parties can arrive a common B-bits secret s by having one party, say party $\mathcal{A}$, transmit δ bits of reconciliation data to party $\mathcal{B}$. We introduce one more integer system parameter c; its relevance will become clear later. We write

$$\langle a+c\rangle_q = s\frac{q}{2^B}+h\frac{q}{2^{B+\delta}}+v \text{ with } 0 \leq h\frac{q}{2^{B+\delta}}+v \leq \frac{q}{2^B}-1 \text{ and } 0 \leq v \leq \frac{q}{2^{B+\delta}}-1. \tag{3}$$

In particular,

$$s = \lfloor \frac{\langle a+c\rangle_q}{(q/2^B)} \rfloor \text{ and } h = \lfloor \frac{\langle\langle a+c\rangle_q\rangle_{q/2^B}}{q/2^{B+\delta}} \rfloor. \tag{4}$$

In the special case that $q = 2^m$, the secret value s corresponds to the B most significant bits of the binary expansion of $\langle a+c\rangle_{2^m}$, h corresponds to the next δ bits, and v corresponds to the $m-B-\delta$ least significant bits.
By considering (1) modulo $\frac{q}{2^B}$, we find that

$$b + c - h\frac{q}{2^{B+\delta}} \equiv v - e \pmod{\frac{q}{2^B}}. \tag{5}$$

As $0 \leq v \leq \frac{q}{2^{B+\delta}} - 1$ and as (2) is satisfied, we have that

$$0 \leq v - e - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}} \leq \frac{q}{2^B} - 1. \tag{6}$$

Combining (5) and (6) we conclude that

$$v - e - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}} = \langle b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}}\rangle_{q/2^B}. \tag{7}$$

By combining (1) and (3), we infer that

$$s\frac{q}{2^B} \equiv b + c - h\frac{q}{2^{B+\delta}} - (v - e) \pmod{q}, \tag{8}$$

and so

$$s \equiv \frac{b + c - h\frac{q}{2^{B+\delta}} - (v - e)}{q/2^B} \pmod{2^B} \tag{9}$$

Combining (9) and (7), and the fact that $s \in [0, 2^B)$, we infer that

$$s = \langle \lfloor \frac{b + c - h\frac{q}{2^{B+\delta}} - \frac{q}{2^{B+\delta+1}} + \frac{q}{2^{B+1}}}{q/2^B} \rfloor \rangle_{2^B}. \tag{10}$$

By simplifying (10), we infer that $\mathcal{B}$ can compute s as

$$s = \langle \lfloor \frac{b+c}{q/2^B} - \frac{h}{2^\delta} - \frac{1}{2^{\delta+1}} + \frac{1}{2} \rfloor \rangle_{2^B}. \tag{11}$$

Equations (10) and (11) show that s can be computed from b, h and the systems parameters q, B and δ. So if party $\mathcal{A}$ sends h to $\mathcal{B}$, then party $\mathcal{B}$ can retrieve s, which can be used a common secret. As (3) implies that $0 \leq h\frac{q}{2^{B+\delta}} < \frac{q}{2^B}$, it follows that $0 \leq h < 2^\delta$, so h can be represented with δ bits.

We note that if $c = 0$, Equation (4) states that the secret s equals the quotient of a and $(q/2^B)$, rounded downwards to the closest integer. With the choice $c = q/2^{B+1}$, the secret s equals the quotient of a and $q/2^B$, rounded to the *closest* integer (modulo 2^B) (and rounded upwards in case of a tie, that is, if a is of the form $k\frac{q}{2^B} + \frac{q}{2^{B+1}}$ for some integer k). With the choice $c = q/(2^{B+1}) - 1$, the secret s equals the quotient of a and $q/2^B$, rounded to the closest integer modulo 2^B, with rounding downwards in case of a tie. Obtaining the secret s as the closest integer to a/q^{B+1} is done in previous work [1], [2].

We again note that in case that $q = 2^m$, the common secret s consists of the B most significant bits of $a+c$; the helper data h consists of the subsequent δ bits of $a+c$. As a consequence, if a is uniformly distributed, then the common secret s given the helper data h is uniformly distributed as well. That is, an adversary cannot obtain information on the common secret s from the observation of the helper data h.

Relation with previous work

For $\delta = 1$ and $q = 2^m$, and obtaining the secret s as the integer closest to the quotient of a and 2^{m-B} (that is, taking $c = 2^{m-B-1}$), our method reduces to the extension of Peikert's scheme from [2]: one reconciliation bit is sent, and the parties agree on an B-bits secret whenever[1] $|e| \leq 2^{m-B-2}$. If $q = 2^m$ and $\delta = m-B-1$, the parties agree on an B-bits secret whenever $|e| \leq 2^{m-B-1}-1$. In the latter case, Peikert's method would only guarantee agreement on an $B-1$-bits secret. *By increasing the number of reconciliation bits, the parties thus can agree on a secret value that is one bit longer.*

Numerical examples

In [2], the authors describe a quantum-secure key exchange method. One party sends to another party a small seed and an $n \times \overline{n}$ matrix with elements from $\mathbb{Z}_q$. In response, an $\overline{m} \times n$ matrix and a binary $\overline{n} \times \overline{m}$ matrix with reconciliation bits are sent. The parties both construct an $\overline{n} \times \overline{m}$ matrix; from each entry of said matrix, B common bits are extracted. The total number of extracted bits (termed key length in the tables below) thus equals $\overline{n} \cdot \overline{m} \cdot B$, while the total number of transmitted bits equals

$$n(\overline{n} + \overline{m})\lceil \log_2(q) \rceil + \overline{m} \cdot \overline{n}.$$

Table 1 is a condensed version of the proposed instantiations in [2, Table 2].

According to [2, Claim 3.2], in case that one reconciliation bit is sent, it is guaranteed that the parties agree on a common B-bits secret if their numbers differ less than 2^{m-B-2} (where m is such that $q = 2^m$). The results from the previous section show that under the same condition, the two parties can agree

[1] The condition from [2, Claim 3.2] is in fact a little stronger: it requires that $|e| < 2^{m-B-2}$

Scheme	n	q	B	$\overline{n}$	$\overline{m}$	key length $= B \cdot \overline{n} \cdot \overline{m}$	**Bandwidth**
Challenge	352	2^{11}	1	8	8	64	7.57 KB
Classical	592	2^{12}	2	8	8	128	14.22 KB
Recommended	752	2^{15}	4	8	8	256	22.57 KB
Paranoid	864	2^{15}	4	8	8	256	25.93 KB

Table 1: Parameter choices from Frodo

on a $B+1$ bits secret if $\delta = m - B - 2$ reconciliation bits are sent. The amount of reconciliation data thus equals $\log_2(q) - B - 2$ bits per matrix entry, and the total required bandwidth equals

$$\log_2(q)n(\overline{n} + \overline{m}) + \overline{m} \cdot \overline{n} \cdot (\log_2(q) - B - 2).$$

As the amount of bits that is agreed on is one larger than in [2], we can reduce $\overline{n}$ and/or $\overline{m}$ and thus reduce overall bandwidth usage. We obtain the results in Table 2. The final column is the ratio of the required bandwidth with the proposed reconciliation scheme and that of the equivalent Frodo system.

Scheme	n	q	B	$\overline{n}$	$\overline{m}$	key length $= B \cdot \overline{n} \cdot \overline{m}$	**Bandwidth**	**Bandwidth ratio**
Challenge	352	2^{11}	2	6	6	72	5.84 KB	0.76
Classical	592	2^{12}	3	7	7	147	12.48 KB	0.88
Recommended	752	2^{15}	5	7	8	280	21.22 KB	0.94
Paranoid	864	2^{15}	5	7	8	280	24.37 KB	0.94

Table 2: Improvement by our reconciliation scheme

We attempted to have $\overline{n} \approx \overline{m}$ to have symmetry in the protocol. If symmetry is a strict requirement, we cannot gain anything with the "Recommended" and "Paranoid" scheme, as $5 \times 7 \times 7$ is smaller than the required key size (256).

Additional remarks

After publication of the first version of this manuscript, Léo Ducas pointed out that Ding [3][2] had described an approximate key agreement scheme, combined with (single-bit) reconciliation, prior to [1]. For a comparison of Ding's and Peikert's method, we refer to [4, p.2].
An even earlier example of sending reconciliation data to obtain exact key agreement can be found in [5, Sec 3.3]. The scheme from [5] has been broken by Albrecht *et al* in [6].

[2]Later and revised versions list Xie and Xie and Lin as co-authors

References

[1] C. Peikert, "Lattice Cryptography for the Internet", *Post Quantum Cryptography*, Proceedings of the 6th Workshop on Post-Quantum Cryptography, PQ Crypto 2014, Springer LNCS, Vol. 8772, 2014, pp. 197-219.

[2] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan and Douglas Stebila, "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE", IACR Cryptology ePrint Archive, Report 2016/659, https://eprint.iacr.org/2016/659.

[3] J. Ding, "A simple provably secure key exchange scheme based on the learning with errors problem", IACR Cryptology ePrint Archive, Report 2012/688, https://eprint.iacr.org/2012/688.

[4] E. Alkim, L. Ducas, Th. Pöppelmann and P. Schwabe, "NEWHOPE without reconciliation", IACR Cryptology ePrint Archive, Report 2016/1157, https://eprint.iacr.org/2016/1157.

[5] W. Zhang, M. Tran, S. Zhu and G. Cao, "A random perturbation-based scheme for pairwise key establishment in sensor networks", MobiHoc'07, pp. 90-99.

[6] M. Albrecht, C. Gentry, S. Halevi and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"", CCS'09, pp. 1-10.