Tatra Mt. Math. Publ. **33** (2006), 113–122

Tatra Mountains
Mathematical Publications

EFFICIENCY CONSIDERATIONS IN UNCONDITIONALLY SECURE COMMUNICATION BY PUBLIC DISCUSSION

Michal Ren

ABSTRACT. Using noisy communication channels, and assuming that the enemy does not have access to the same information as the legitimate parties allows for an unconditionally secure key exchange protocol proposed by [Maurer U. M.: *Secret key agreement by public discussion from common information*, IEEE Trans. Inform. Theory, **39** (1993) 733–742]. The main result of this paper is the analysis of Maurer's multi-round protocol [Maurer U. M.: *Protocols for secret key agreement by public discussion based on common information*, Advances in Cryptology, CRYPTO '92, Lecture Notes Comput. Sci., Springer-Verlag, Berlin, Vol. 740, 1993, pp. 461–470], and the proof that for any choice of protocol parameters the optimal round length is always two. In addition, some remarks are made about protocols with communication channels of non-binary distributions.

1. Maurer's noisy channel protocol

First, let us review Maurer's basic protocol [1], and provide proof of Maurer's statement in [1] that the presented protocol makes it possible to gain an advantage over Eve even with communication equipment worse than hers.

Let us assume that all the parties are receiving a satellite transmission that is very weak—so weak that the signal to noise ratio is extremely poor, and the transmission cannot be received completely without errors even by using exceptionally good equipment. The satellite should have its own source of randomness, and use it to generate the bits that it sends out.

With these assumptions, Alice, Bob and Eve know random variables, X, Y and Z that are the result of sending a random bit (which is 0 or 1 with probability of $\frac{1}{2}$) through three independent communication channels that have error probabilities of e_A, e_B and e_E, respectively. Of course $e_A, e_B, e_E \in (0, 0.5)$,

2000 Mathematics Subject Classification: 94A60.
Keywords: unconditional security, public discussion, broadcast channel, privacy amplification, public randomness, key exchange.

since error probabilities cannot be equal to zero (we are assuming a noisy channel), nor reach 0.5 (otherwise the channel would consist exclusively of noise).

Notice that

$$P_{XYZ|R} = P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R}\,,$$
$$P_{XYZ}(x, y, z) = P_{XYZ}(\bar{x}, \bar{y}, \bar{z})\,.$$

Let us assume that Alice and Bob want to share a bit, so that Eve's knowledge about it is lesser than theirs. Alice can generate a random bit, with probability $\frac{1}{2}$, and send to Bob the result of xoring several bits received from satellite—$X_1, X_2, \ldots, X_N$ and her generated bit. Bob accepts the bit only if, after xoring with $Y_1, Y_2, \ldots, Y_N$, he received a block of zeroes or ones. In other words, Alice and Bob communicate by repeat code of length N.

Assuming that Alice's random bit that she wanted to agree on with Bob was 0, let α_{rs} denote the probability that for a certain, single bit in the message, Bob will think it was r, and Eve—s. Then

$$\alpha_{00} = (1 - e_A)(1 - e_B)(1 - e_E) + e_A e_B e_E\,,$$
$$\alpha_{01} = (1 - e_A)(1 - e_B)e_E + e_A e_B(1 - e_E)\,,$$
$$\alpha_{10} = (1 - e_A)e_B(1 - e_E) + e_A(1 - e_B)e_E\,,$$
$$\alpha_{11} = (1 - e_A)e_B e_E + e_A(1 - e_B)(1 - e_E)\,.$$

Bob might accept both correct and incorrect messages; the respective probabilities are

$$P_{\text{correct}} = \big((1 - e_A)(1 - e_B) + e_A e_B\big)^N,$$
$$P_{\text{incorrect}} = \big(1 - (1 - e_A)(1 - e_B) - e_A e_B\big)^N.$$

Bob accepts the message only in those two cases, so the acceptance probability will be the sum $P_{\text{acc}} = P_{\text{correct}} + P_{\text{incorrect}}$. Therefore the channel from Alice to Bob corresponds to a binary channel with error probability β.

$$\beta = \frac{P_{\text{incorrect}}}{P_{\text{acc}}}\,.$$

Let p_w, with $0 \leqslant w \leqslant N$, denote the probability that when Alice has sent a zero codeword $[0, 0, \ldots, 0]$ to Bob, he accepted, and Eve has received a codeword of Hamming weight w (that is—containing w ones)

$$p_w = \alpha_{00}^{N-w}\, \alpha_{01}^{w} + \alpha_{10}^{N-w}\, \alpha_{11}^{w}\,.$$

Assuming that Eve guesses optimally, then average probability that she made an error is (for odd N)

$$\gamma = \frac{1}{P_{\text{acc}}} \sum_{w=\lceil N/2 \rceil}^{N} \binom{N}{w} p_w\,.$$

We will show that one can always choose an odd N so large that $\gamma > \beta$, even if e_E is significantly smaller than e_A and e_B, which means that Bob will have more information about the bit sent by Alice than Eve if he accepts the message.

We will prove that for a sufficiently large N, $\beta < \gamma$. Clearly, $\beta < \gamma$ is equivalent to

$$\left(1-(1-e_A)(1-e_B)-e_Ae_B\right)^N < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \left(\alpha_{00}^{N-w}\alpha_{01}^{w}+\alpha_{10}^{N-w}\alpha_{11}^{w}\right). \quad (1)$$

Notice that

$$P_{\text{incorrect}} = \left(1-(1-e_A)(1-e_B)-e_Ae_B\right)^N = (\alpha_{10}+\alpha_{11})^N,$$

and so it follows that (1) holds if for sufficiently large N

$$\sum_{w=0}^{N} \binom{N}{w} \left(\alpha_{10}^{N-w}\alpha_{11}^{w}\right) < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \left(\alpha_{00}^{N-w}\alpha_{01}^{w}+\alpha_{10}^{N-w}\alpha_{11}^{w}\right).$$

We can assume, without loss of generality, that Alice's error rate e_A is the same as Bob's e_B. If they are different, they can be trivially made equal by artificially introducing errors to bring the lower error rate to the desired level. This assumption simplifies calculations; in particular, in this case $\alpha_{10} = \alpha_{11}$, and (1) becomes

$$\sum_{w=0}^{N} \binom{N}{w} \alpha_{11}^{N-w}\alpha_{11}^{w} < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \left(\alpha_{00}^{N-w}\alpha_{01}^{w}+\alpha_{11}^{N-w}\alpha_{11}^{w}\right),$$

i.e.,

$$\sum_{w=0}^{N} \binom{N}{w} \alpha_{11}^{N} < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \alpha_{00}^{N-w}\alpha_{01}^{w} + \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \alpha_{11}^{N}.$$

After simplifying, we obtain that under the assumption $\alpha_{10} = \alpha_{11}$, (1) is equivalent to

$$(2\alpha_{11})^N < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \alpha_{00}^{N-w}\alpha_{01}^{w} + \frac{1}{2}(2\alpha_{11})^N,$$

and

$$\frac{1}{2}(2\alpha_{11})^N < \sum_{w=\lceil N/2\rceil}^{N} \binom{N}{w} \alpha_{00}^{N-w}\alpha_{01}^{w}.$$

We can decrease the right side of the inequality, and take into account only one of the summands. Therefore to prove (1) it is sufficient to prove that

$$\frac{1}{2}(2\alpha_{11})^N < \binom{N}{\lceil N/2\rceil}\alpha_{00}^{N-\lceil N/2\rceil}\alpha_{01}^{\lceil N/2\rceil}. \tag{2}$$

Note that when we increase N by 2, the left side of 2 grows $4\alpha_{11}^2$ times. The right side grows, with sufficiently large N, $4\alpha_{00}\alpha_{01}$ times, because

$$\binom{N+2}{\lceil N/2\rceil+1}\Big/\binom{N}{\lceil N/2\rceil} \longrightarrow 4\,.$$

So, it is enough to show that $\alpha_{11}^2 < \alpha_{00}\alpha_{01}$—then it will be obvious that the right side grows faster, and with sufficiently large N, the inequality (2) will be satisfied.

Since always $\alpha_{00}\alpha_{01} - \alpha_{10}\alpha_{11} = (1-2e_A)(1-2e_B)(1-e_E)e_E$, with $0 < e_A = e_B < 0.5$ and $0 < e_E < 0.5$, it follows that indeed $\alpha_{11}^2 < \alpha_{00}\alpha_{01}$, and so the inequality (2) is satisfied for sufficiently large N.

2. Multi-round protocol

Sending long blocks in the protocol above is very inefficient, as the probability that the block is accepted becomes very small, and many retries are necessary. An enhancement was proposed by Maurer in [2] where Alice and Bob communicate in multiple rounds. In this section, we will review Maurer's multi-round protocol [2], and give a detailed explanation why error rates are the same as in single-round protocol.

Alice and Bob are assumed to initially share an unreliable string (meaning that they have different readings of it—for instance, after they receive data unreliably from a satellite). Instead of Alice sending very long blocks of this string xored with also zeroes or ones, and hoping for Bob to accept, they do the following:

- Alice randomly chooses a bit as before.
- Alice copies the bit n times, where n is the round length, and xors the resulting string with n first bits of the string that she shares with Bob.
- Alice sends the result to Bob.
- Bob accepts the block as before—depending on whether after xoring it with his n first bits of the shared string, he got all zeroes or ones; otherwise he rejects it.
- Alice and Bob discard the first n bits of the shared string.

- If the block was accepted:
  - Alice appends the random bit she chose to a new string.
  - If Bob got all ones, he appends a one to a new string, and if he got all zeroes—he appends a zero.

This procedure is repeated until there are no bits left in the shared string. Now Alice and Bob are again in possession of a new shared string, which is much shorter than the one they had at the beginning (at least n times shorter, and more if Bob rejected some blocks—on average it will be $n/P_{\text{acc}}(n)$ times shorter, where $P_{\text{acc}}(n)$ is the probability of accepting an n-bit block). However, this loss was turned into an increase in reliability.

Alice and Bob repeat this shrinking of the string in rounds, with every round starting with the shared string being the result of the one before. Let us assume that they executed k rounds, and finished with 1 shared bit. Then the protocol was essentially the same as the basic repeat-block one (the one without rounds), with block length of $N = n^k$. It is easy to see if one considers how the parts of the original string affect the final bit that was exchanged. There will be a lot of n-bit blocks in the first string that Bob has accepted. Most of them will not affect the final bit at all, as in the later rounds they make up a block that will get rejected. We will consider only those that do affect the final bit (there will be n^{k-1} of them). Let us first look at n of those n-bit blocks. They make up one block in the string in the second round. Rejection of this block would mean that some of the blocks from the first round were accepted correctly, and some were accepted incorrectly. Since we are considering only the blocks that affect the final bit, we know that Bob has accepted. Therefore either all the bits in n n-bit blocks from the first round are received correctly, or they are all received incorrectly. By continuing this reasoning and extending it into all n^{k-1} n-bit blocks from the first round, we arrive at the conclusion that after k rounds, the n^k bits that affect the final exchanged bit were either all received correctly or incorrectly. This is exactly the same situation as in the case of the previous protocol. The error probabilities β and γ will therefore be the same, as will Alice's knowledge about Alice and Bob's secret—in both cases Eve knows that they agreed on all the bits necessary to share one bit. However, with multiple rounds, Alice and Bob were able to selectively use the "good" parts of the string, instead of rejecting the whole N-bit block if even one bit does not match. This lets them use up much less bits on average.

3. Optimal round length

First, let us note that for given error rates e_A, e_B, e_E, the choice of N determines β and γ. Also note that the multi-round version with $n^k = N$ has exactly the same error probabilities β and γ as the single-round version with block of length N, which follows directly from the description in the previous section. We may therefore assume that the participants will choose an N suitable to their situation, and e_A, e_B, e_E.

Let us choose an N as the block size for the repeat-block protocol. Let $P_{\mathrm{acc}}(N)$ denote the probability of accepting the round of length N. We want to maximize the ratio of the expected number of bits used up to share one bit in the repeat-block protocol, to the number of bits in the multi-round protocol. The average number of tries necessary for acceptance can be calculated from geometric distribution with probability of success $p = P_{\mathrm{acc}}(N)$ in the repeat-block protocol, and $p = P_{\mathrm{acc}}(n)$ in a single round of the multi-round protocol. Therefore the average number of bits used up in the repeat-block protocol to share one bit will be $\frac{N}{P_{\mathrm{acc}}(N)}$. The average number of bits required to share one bit in a single round of the multi-round protocol will be $\frac{n}{P_{\mathrm{acc}}(n)}$, and because we need k rounds, the total average number of bits used up to share one bit will be $\left(\frac{n}{P_{\mathrm{acc}}(n)}\right)^k$.

Theorem 1. *For any given error rates e_A, e_B, e_E, and for any choice of N (which determines β and γ), the choice of round length of two ($n = 2$) results in maximum possible ratio $\left(\frac{N}{P_{\mathrm{acc}}(N)}\right)/\left(\frac{n}{P_{\mathrm{acc}}(n)}\right)^k$, which determines the number of bits used in the multi-round protocol to exchange one bit.*

Proof. We want to maximize:

$$\frac{N \cdot P_{\mathrm{acc}}(n)^k}{n^k \cdot P_{\mathrm{acc}}(N)} \longrightarrow \max .$$

Note that $P_{\mathrm{acc}}(n) = c^n + (1-c)^n$, where c is a constant, $0 < c < 1$, and that $N = n^k$. We can simplify to:

$$\frac{\left(c^n + (1-c)^n\right)^k}{c^N + (1-c)^N} \longrightarrow \max ,$$

$$\frac{\left(c^n + (1-c)^n\right)^{\log_n N}}{c^N + (1-c)^N} \longrightarrow \max .$$

The choice of N and n determine k—it is $k = \log_n N$. Also note that the denominator is a constant (with a fixed N), so we can omit it:

$$\left(c^n + (1-c)^n\right)^{\log_n N} \longrightarrow \max .$$

It can be verified by calculus that the smallest n gives the biggest improvements in the amount of bits that the protocol uses up. Since the smallest amount of bits we can pick is two, it follows that a protocol with round length equal to two is always the most efficient in the binary symmetric channel case. □

4. A note about unauthenticated channels

We have assumed that the channel between Alice and Bob is authenticated. This is a luxury seldom achieved. A protocol for authentication is necessary—one that is provably secure; otherwise there is no point in using a quite inefficient unconditionally secure protocol for key generation. There exist simple provably secure protocols for message authentication [6]. However, they require a certain amount of shared bits for every authenticated message. In general, if a protocol is secure against passive adversaries, there also exists a protocol secure against active ones, provided that Alice and Bob share a secret key in the beginning [5]. We will show that a very simple construction, based on the multi-round protocol above, and mentioned in [1], is secure against active adversaries.

Alice and Bob can use an authentication protocol based on universal hashing [6] to authenticate all exchanged messages by sending an authenticator to the other party, created by using a shared key.

It follows directly from [6] that

Fact 4.1 (Stinson [6]). *For a-bit long message there exists an authentication protocol with authenticators of length b with attack success probabilities of*

- *by impersonation (introducing a new message)* $P_i = 2^{-b}$,
- *by substitution (changing a valid message)* $P_s = 2^{-b} \cdot (\log a - \log b + 1)$,

and with key length of $b \cdot (\log a - \log b + 2)$.

Proof. The proof is straightforward from [6]—one constructs an $\varepsilon - ASU_2$ family of $2^{b \cdot (\log a - \log b + 2)}$ hash functions from a set of size 2^a to the set of size 2^b, such that $\varepsilon = 2^{-b} \cdot (\log a - \log b + 1)$. The attack success probabilities then follow from [6].

We know that $|B| = q = 2^b$, and $|A| = 2^a$. We also know that $|A| = q^{2^i}$. Therefore

$$\begin{aligned} q^{2^i} &= 2^a, \\ 2^{b \cdot 2^i} &= 2^a, \\ b \cdot 2^i &= a, \\ 2^i &= \frac{a}{b}, \\ i &= \log \frac{a}{b} = \log a - \log b. \end{aligned} \tag{3}$$

From [6] with $q = 2^b$ and $i = \log a - \log b$ it further follows that:

$$|H| = q^{i+2} = 2^{b \cdot (\log a - \log b + 2)},$$

and

$$\varepsilon = \frac{i+1}{q} = 2^{-b} \cdot (\log a - \log b + 1)\,.$$

□

It is obvious that even very ineffective key generation protocol can be authenticated with unconditional security. More formally:

Theorem 2. *For given probabilities P_i and P_s, round acceptance probability P_{acc}, and round length N there exists a key generation protocol with authentication which requires less shared secret than it produces.*

The proof follows directly from Fact 4.1, since the length of the secret which is used up rises proportionally to the logarithm of the amount of generated bits. Thus, with sufficiently large amount, more will be generated than consumed.

5. Non-binary signal distributions

In nature, no signal is truly binary. For example, the normal distribution of signal strength would be closer to reality than the binary one. One can exploit this by using the signal value, as seen by the receiver before it is digitized. In normal distribution model it is assumed that the random bit server sends out a signal with normal distribution, centered around zero, with all positive values interpreted as a binary one, and all negative ones as zero. Alice and Bob receive the signal with a random value (noise) added to the signal, also with normal distribution, centered around zero. Eve also receives the signal with a random value, with normal distribution, but of lower standard deviation than Alice and Bob.

Alice and Bob accept the signal only when the value they see is a certain number of standard deviations away from zero. They then communicate in order to agree on bits that they both received with high reliability (i.e., which were far from zero).

There is a lot of parameters, and it is difficult to find the error probabilities analytically, so let us look at an example:

We will compare Maurer's original (repeat-block) protocol with the following parameters: $N = 32$, $e_A = 0.35$, $e_B = 0.35$, $e_E = 0.15$. Since the probability of Bob accepting a 32-bit block is only $\approx 3.7 \cdot 10^{-9}$, the average number of random bits used to achieve Alice and Bob's error probability $\beta \approx 0.3\ \%$, and Eve's $\gamma \approx 1.9\ \%$, is about $8.7 \cdot 10^{9}$.

For the multi-round protocol, we will pick round length of 2. The number of rounds will have to be 5, since $2^5 = 32$. However, since the probability of accepting a block of length 2 is almost $30\ \%$, the average amount of necessary random bits will be only about $1.4 \cdot 10^4$.

We will pick parameters for the normal distribution case, so that the error probabilities are similar: random source will have standard deviation of 1, Alice's, Bob's, and Eve's equipment—$2, 2$, and 0.5 respectively. Error probabilities will then be approximately 0.35, 0.35, and 0.15 respectively. If we have Alice and Bob accepting only if the received signal is at least 10.5 standard deviations away from zero, they will use on average less than $8 \cdot 10^9$ bits. Their error probability will be about $9.5 \cdot 10^{-15}$, while Eve's—$1.9 \cdot 10^{-14}$.

While it is obviously difficult to compare different models, it is worth noting that the normal distribution model can be a good starting point for a multi-round construction, similar to the enhancement of Maurer's protocol. Also, for comparable choices in other parameters, bit error probabilities are much lower, decreasing the need for error correction (which can be dangerous, as it is easy to increase Eve's information too much). In addition, a model in which the random source produces a signal with normal distribution can be useful if protocol participants are using deep space radio source. This is preferable to manmade installations, as the random bit source should always be located somewhere inaccessible. Otherwise, if the attacker can move closer to it, his signal strength can become orders of magnitude higher.

A more practical advantage of the model in which receiver outputs a signal with normal distribution (or any distribution which allows to reject signals that are too uncertain) is that it greatly reduces the amount of communication between Alice and Bob, as they can ignore the bits whose values they are not sufficiently sure of. This advantage can be exploited regardless of the random source's distribution; in particular it could be binary, as in the previous examples. In general, since it is generally easier not to convert an analog signal to a digital one, there seems to be no particular disadvantage to building non-binary receivers.

Conclusion

The presented protocol is efficient enough to be used in practical applications, provided that certain assumptions about the quality of receiving equipment are true. However, with quantum cryptography becoming cheaper, its main advantage is that it could be used over longer distances, likely with a deep space object as a radio source.

Acknowledgements. I would like to thank my advisor, Professor Jerzy Jaworski for his invaluable support and advice in writing this paper.

This paper was supported as a research project by KBN grant 0 T00A 003 23 (2002–2005).

REFERENCES

[1] MAURER, U. M.: *Secret key agreement by public discussion from common information*, IEEE Trans. Inform. Theory **39** (1993), 733–742.

[2] MAURER, U. M.: *Protocols for secret key agreement by public discussion based on common information*, in: Advances in Cryptology, CRYPTO '92, Lecture Notes in Comput. Sci., Vol. 740, Springer-Verlag, Berlin, 1993, pp. 461–470.

[3] MAURER, U. M.—WOLF, S.: *Privacy amplification secure against active adversaries*, in: Advances in Cryptology, CRYPTO '97, Lecture Notes in Comput. Sci., Vol. 1294, Springer-Verlag, Berlin, 1997, pp. 307–321.

[4] MAURER, U. M.—WOLF, S.: *Unconditionally secure key agreement and the intrinsic conditional information*, IEEE Trans. Inform. Theory **45** (1999), 499–514.

[5] MAURER, U. M.—WOLF, S.: *Secret key agreement over a non-authenticated channel*, IEEE Trans. Inform. Theory **49** (2003), 822–831.

[6] STINSON, D. R.: *Universal hashing and authentication codes*, in: Advances in Cryptology, CRYPTO '91, Lecture Notes in Comput. Sci., Vol. 576, Springer-Verlag, Berlin, 1992, 74–85.

Received October 15, 2004

Faculty of Mathematics and Computer Science
Adam Mickiewicz University of Poznań
ul. Umultowska 87
PL–61-614 Poznań
POLAND

E-mail: renmich@amu.edu.pl