

Quantum-Inspired Secure Wireless Communication Protocol Under Spatial and Local Gaussian Noise Assumptions

Masahito Hayashi

IEEE Access, vol. 10, 29040-29068 (2022).

Shenzhen Institute for Quantum Science and Engineering,

Southern University of Science and Technology

Shenzhen International Quantum Academy

Graduate School of Mathematics, Nagoya University



南方科技大学

SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY



NAGOYA UNIVERSITY

空间和局部高斯噪声假设下的量子启发的安全无线通信协议

IEEE Access, vol. 10, 29040-29068 (2022).

林 正人

南方科技大学/量子科学与工程研究院

(深圳)国际量子研究院

名古屋大学 多元数理科学研究科



南方科技大学

SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY



NAGOYA UNIVERSITY

空間和局部高斯雜訊假設下的量子啓發 的安全無線通訊協定

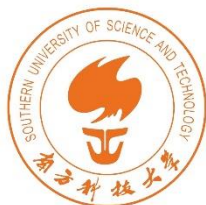
IEEE Access, vol. 10, 29040-29068 (2022).

林 正人

南方科技大學/量子科學與工程研究院

(深圳)國際量子研究院

名古屋大學 多元數理科學研究科



南方科技大學
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

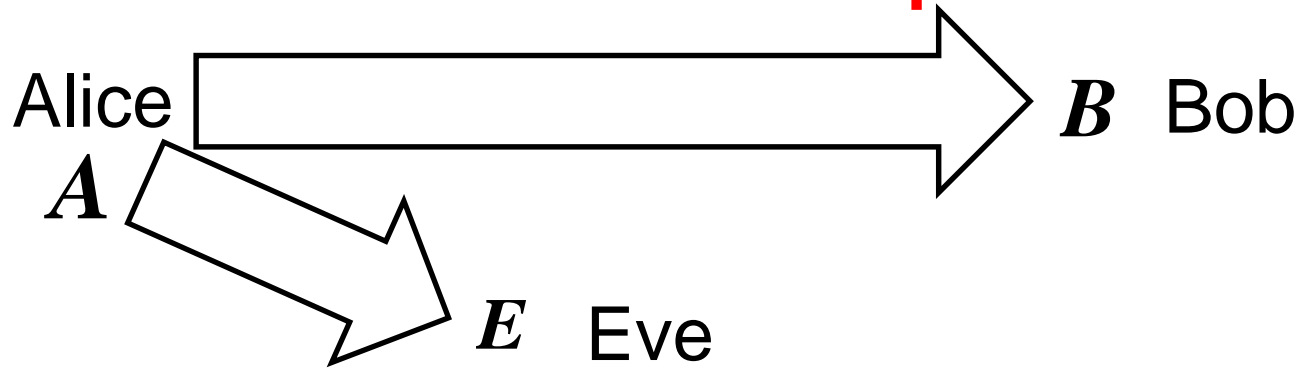


NAGOYA UNIVERSITY

Contents

- Our model
- Assumptions
- Purpose
- Multi-antenna attack
- Mathematical structure
- Interference model
- Full protocol
- Calculation complexity
- Security evaluation (including numerical calculation)
- Conclusion

Problem in wire-tap channel



To apply wire-tap channel model, we need the condition

$$I(A;B) > I(A;E)$$

To realize this condition, physically Bob needs to be closer to Alice than Eve.

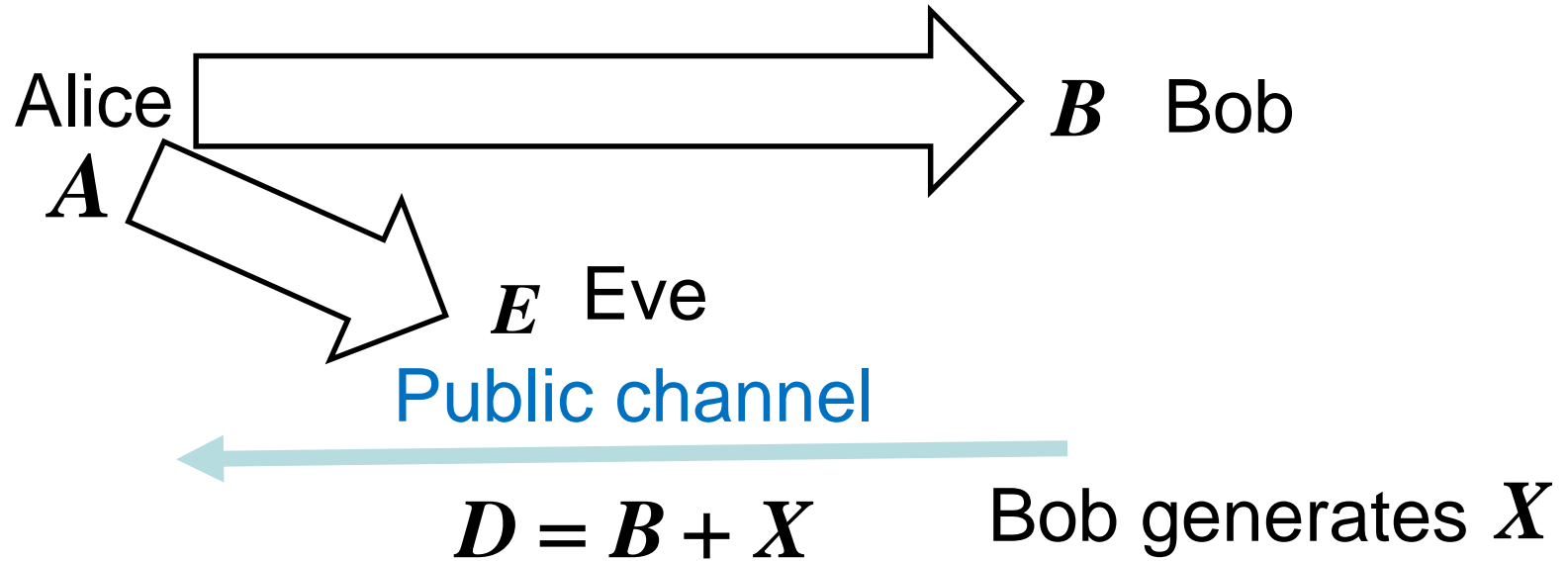
However, usually, Eve is stronger than Bob.

Even if $I(A;B) < I(A;E)$,

If their noises are independent, $I(A;B) > I(B;E)$

we can generate secure keys via reverse information reconciliation.

Reverse information reconciliation



$$I(X; A, D) - I(X; E, D) = I(B; A) - I(B; E)$$

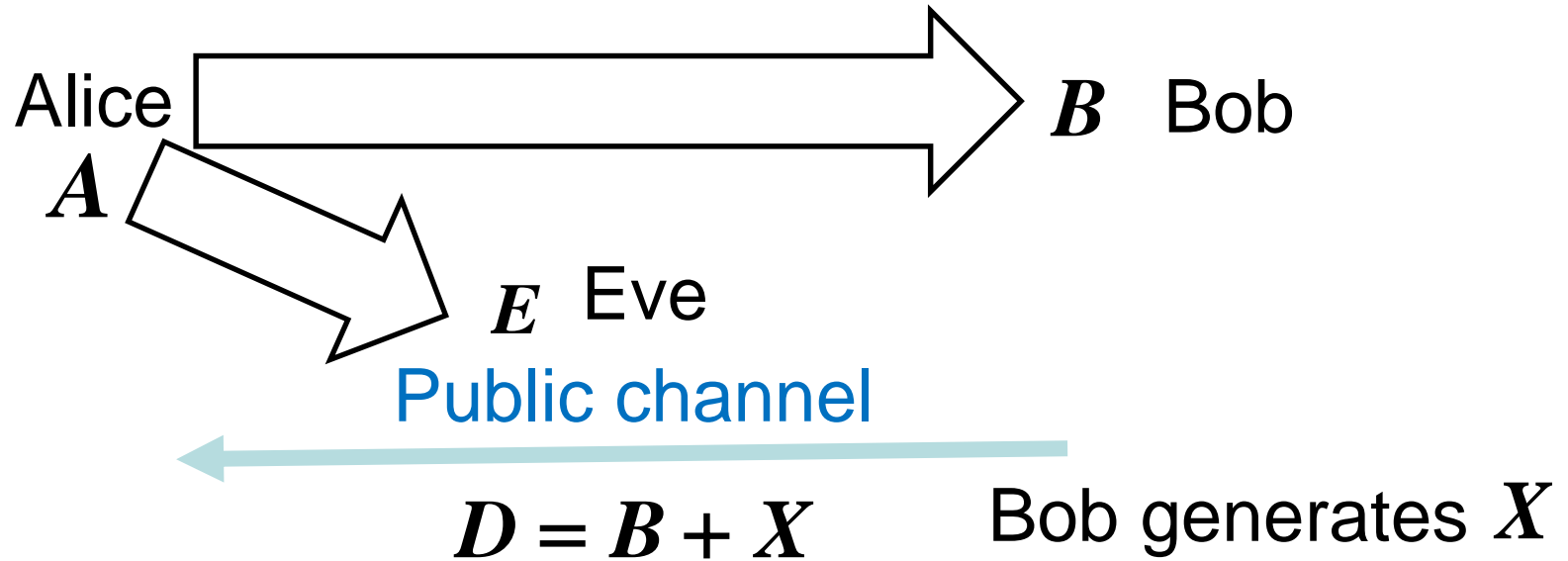
If their channel noises are independent,

$$B - A - E \quad \longrightarrow \quad I(A; B) > I(B; E)$$

MH and A. Vazquez-Castro, "Two-Way Physical Layer Security Protocol for Gaussian Channels," *IEEE Transactions on Communications*, vol. 68, 3068 – 3078 (2020).

MH and A. Vazquez-Castro, "Physical Layer Security Protocol for Poisson Channels for Passive Man-in-the-middle Attack," *IEEE Transactions on Information Forensics and Security*, vol. 15, 2295 – 2305 (2020).

Reverse information reconciliation



$$I(X; A, D) - I(X; E, D) = I(B; A) - I(B; E)$$

If their channel noises are independent,

$$B - A - E \quad \Rightarrow \quad I(A; B) > I(B; E)$$

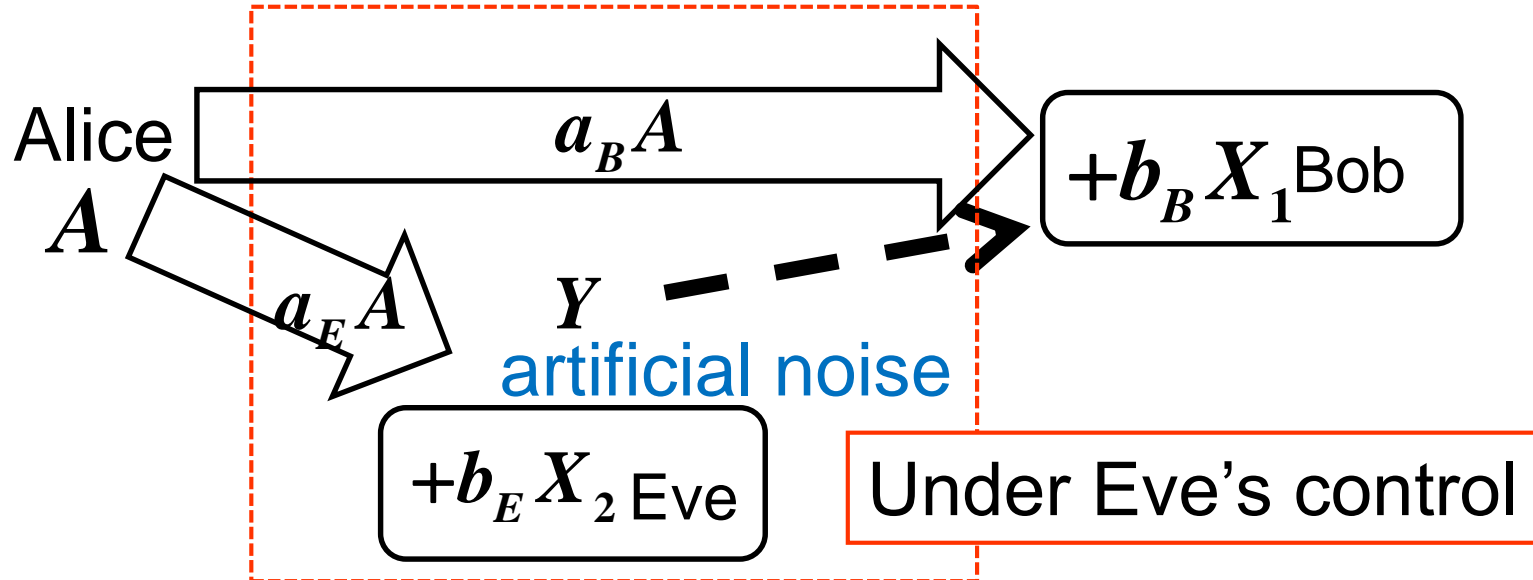
However, if there is interference between Bob's and Eve's channels, or if Eve controls Bob's channel noise, *we cannot say that they are independent.*

Our model

$$E = a_E A + b_E X_2$$

Eve generates artificial noise Y and knows it.

$$B = a_B A + Y + b_B X_1 + e_B$$



This model contains Jamming attack.

Assumptions

(A1) Intermediate space between Alice and Bob might be controlled by Eve.

Eve decides injected noise Y dependently on her previous observations.

(A2: *Local Gaussian noise ass.*) Eve's and Bob's detectors have a Gaussian noise, and Alice and Bob know the lower bounds of the powers of their noise.

(A3: *Spatial ass.*) Alice and Bob know the lower bound of the attenuation for Alice's signal in Eve's detection.

(A4) Wireless communication between Alice and Bob is quasi static. Alice and Bob can make public noiseless communication.

Purpose

- Our aim is to propose a protocol to **generate** quantitatively secure keys between Alice and Bob under a reasonable assumption advantageous to Eve.
- Our aim is not to always generate secure keys, but is to **detect** the existence of eavesdropping with high probability when it exists.
- When they consider that there is no eavesdropper, their keys are required to **be matched and secret**. In other word, it is required to **discard** their keys when an eavesdropper exists.
- This requirement is similar to quantum key distribution (QKD).

Purpose

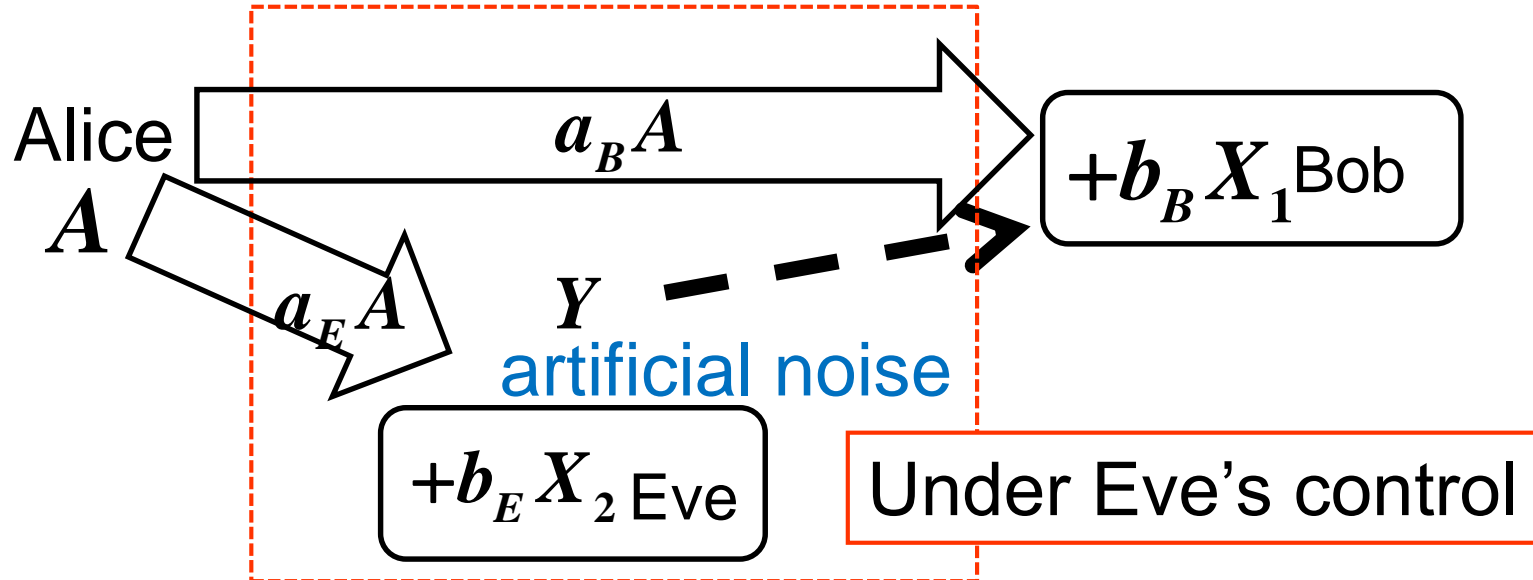
- **Soundness:** The obtained keys should be always correct and secret.
- **Completeness:** When Eve does not exist or Eve's noise injection behaves as natural noise with an acceptable level, we should generate our secure keys. That is, when the iid assumption holds with acceptable noise level, we need to generate our secure keys.
- This requirement is similar to quantum key distribution (QKD).

Noise injecting attack

$$E = a_E A + b_E X_2$$

Eve generates artificial noise Y and knows it.

$$B = a_B A + Y + b_B X_1 + e_B$$



Alice and Bob cannot distinguish whether the noise out of Bob's detector comes from Eve or it is background noise, if Y has a natural behavior.

Parameters

$$E = a_E A + b_E X_2$$

$$B = a_B A + Y + b_B X_1 + e_B$$

Coefficient	Meaning	Long time period behavior	Treatment	Estimation method
a_B	Attenuation	Stochastic	Estimated by sampling	average of $A_i B_i$
a_E	Attenuation	Stochastic	Constant (Upper bound)	distance between Alice and Eve
P_Y	Noise distribution during transmission	Stochastic	Estimated by sampling	Inverse Gaussian conv. $B - a_B A$
b_B	Bob's detector noise amplitude	Constant	Constant	performance of Bob's detector
b_E	Eve's detector noise amplitude	Constant	Constant	performance of Eve's detector

Mathematical structure

$$E = a_E A + b_E X_2$$

Eve generates artificial noise Y and knows it.

$$B = a_B A + Y + b_B X_1 + e_B$$

b_B, b_E : We assume its lower bound

a_B, P_Y : We can estimate by random sampling

a_E : We assume its upper bound by topology

X_i : Subject to independent standard Gaussian distribution.

Theorem

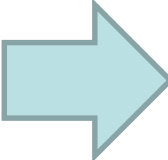
When A is subject to standard Gaussian Eve's information can be reduced to

$$E' := \frac{a_E a_B}{a_E^2 + b_E^2} E + Y + e_B$$

Sketch of proof

$U := b_E A - a_E X_2$ is a Gaussian random variable with variance $b_E^2 + a_E^2$ that is independent of E, X_1, Y

$$A = \frac{a_E}{a_E^2 + b_E^2} E + \frac{b_E}{a_E^2 + b_E^2} U$$

 $B = a_B A + Y + b_B X_1 + e_B$

$$= \frac{a_B a_E}{a_E^2 + b_E^2} E + Y + e_B + \frac{a_B b_E}{a_E^2 + b_E^2} U + b_B X_1$$

$$= E'$$

Eve's information

Independent of
Eve's information

Multi-antenna attack

Eve has k antennas.

$$\mathbf{E}_i = \mathbf{a}_{E,i} \mathbf{A} + \mathbf{b}_{E,i} \mathbf{X}_{2,i} \quad (i = 1, \dots, k)$$


$$\mathbf{B} = \mathbf{a}_B \mathbf{A} + \mathbf{Y} + \mathbf{b}_B \mathbf{X}_1 + \mathbf{e}_B$$

Eve knows \mathbf{Y} .

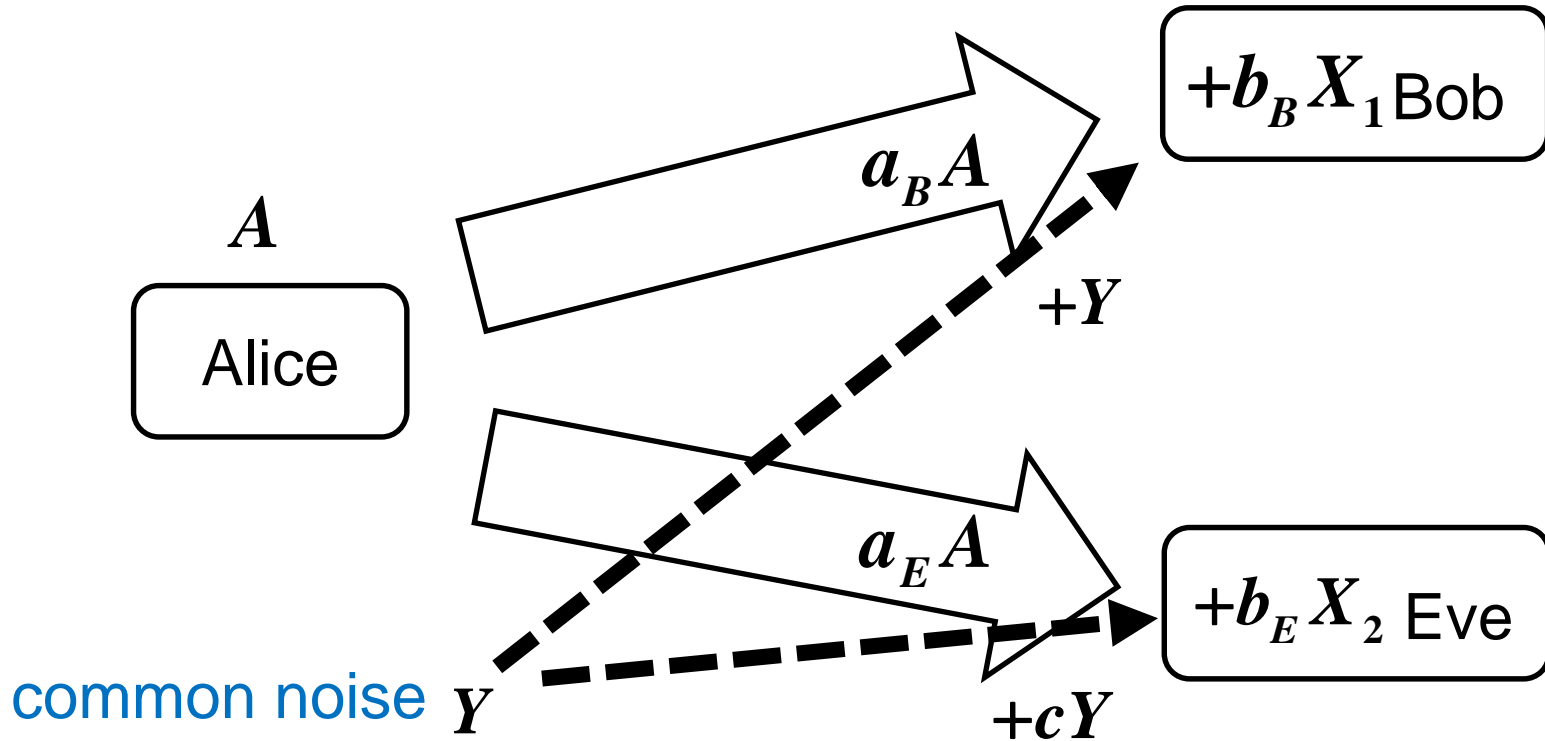
$\mathbf{E}_1, \dots, \mathbf{E}_k$ are converted to $\mathbf{E} := \sum_{i=1}^k \frac{\mathbf{E}_i}{\mathbf{a}_{E,i}}$
and its orthogonal components.

Eve's information can be reduced to

$$\mathbf{E} = k\mathbf{A} + \sum_{i=1}^k \frac{\mathbf{b}_{E,i}}{\mathbf{a}_{E,i}} \mathbf{X}_{2,i} \quad \text{and } \mathbf{Y}$$


$$\mathbf{E} = \mathbf{a}_E \mathbf{A} + \frac{\mathbf{b}_E}{\mathbf{a}_E} \sqrt{k} \mathbf{X}_2 \quad \text{when } \mathbf{a}_{E,i} = \mathbf{a}_E, \mathbf{c}_{E,i} = \mathbf{c}_E$$

Interference model



Eve of interference model is a special case of Eve of noise injection model.

When $c = (a_E^2 + b_E^2) / a_B a_E$, Eve's information is the same as Eve's information of noise injection attack.

Ideas for our protocol

Backward information reconciliation:

When Eve is close to Alice than Bob, forward information reconciliation does not generate secure keys.

Radom sampling:

Alice and Bob randomly select sampling pulses to estimate their channel. This process prevents Eve to change the channel without detecting such an action.

Post selection:

Alice and Bob can select the blocks that are more advantageous to them. So, they can generate secure keys even when the channel noise fluctuates.

Full protocol

Step 1: [Initial key transmission] Alice generates her information according to standard Gaussian distribution and sends it to Bob. She repeats it $n + 2l$ times.

Step 2: [Estimation 1] After initial communication, Alice and Bob randomly choose l -sample data.

They obtain the estimates \hat{a}_B .

Step 3: [Estimation 2] Alice and Bob randomly choose another l -sample data. Based on them, they obtain the estimates $\hat{P}_{B-\hat{a}_B A}$.

Step 4: [Secure key distillation] Based on the above estimates, Alice and Bob apply the backward secure key distillation protocol for n data.

Key distillation protocol

Step 1: [Discretization] Bob converts his random variable $B - \hat{e}_B$ to 1 or -1 by taking the sign of B , i.e., he obtains the new bit random variable $B' := \text{sgn}(B - \hat{e}_B)$ in \mathbb{F}_2

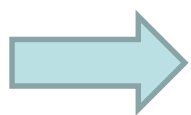
Step 2: [Information reconciliation] Given an error correcting code $C \subset \mathbb{F}_2^n$, Bob computes the syndrome as an element $[B'^n]$ of the coset space \mathbb{F}_2^n / C from his bit sequence B'^n , calculate its representative element $\alpha([B'^n])$ in \mathbb{F}_2^n , and sends $\alpha([B'^n])$ to Alice. Bob calculates $B'^n - \alpha([B'^n]) \in C$.

Alice applies the error correction to the data $((-1)^{\alpha([B'^n])_i} A_i)_{i=1}^n$ so that she obtains the estimate of $B'^n - \alpha([B'^n]) \in C$.

Key distillation protocol

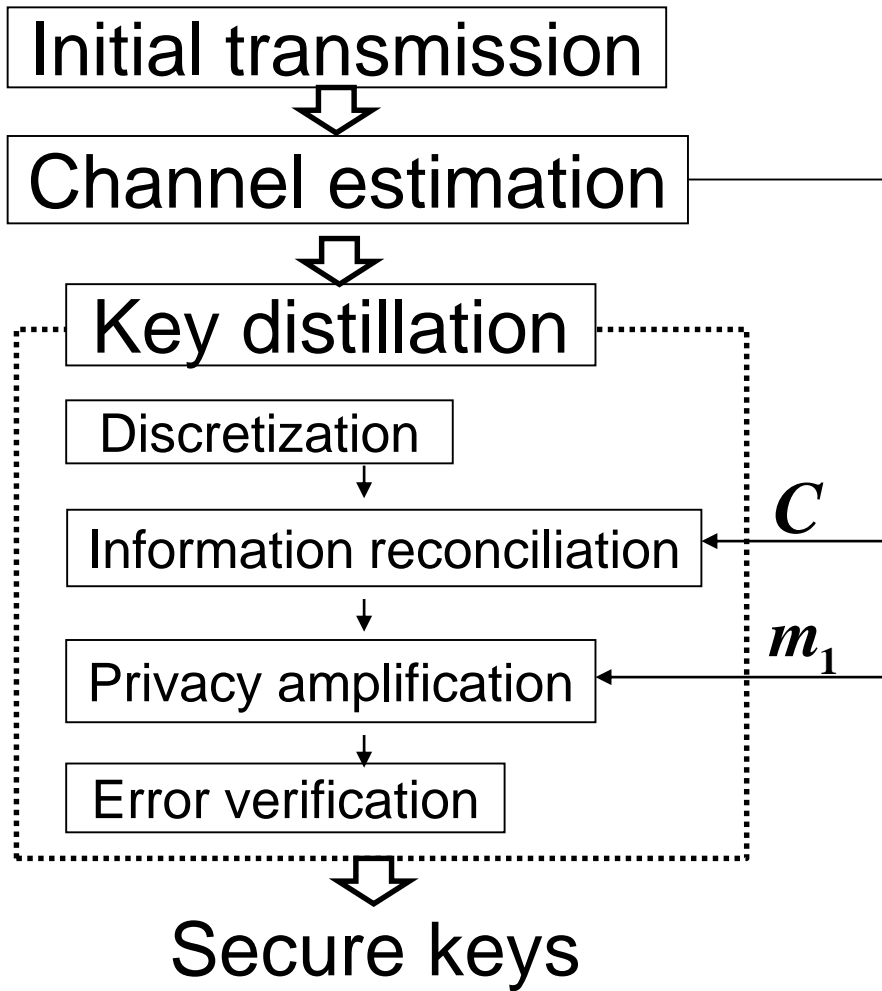
Step 3: [Privacy amplification] Based on estimated values, Alice and Bob decide sacrifice bit length m_1 . Then, they apply universal2 hash function to their bits in \mathbf{C} with sacrifice bit length m_1 . They obtain the keys with length $\dim \mathbf{C} - m_1$. Here, Alice (or Bob) generates the random seeds locally and sends it to Bob (or Alice) via public channel.

Step 4: [Error verification] Alice and Bob choose the bit length m_2 for error verification. They apply another universal2 hash function to the keys with output length m_2 . They exchange their output of the universal2 hash function. If they are the same, discarding their final m_2 bits from their keys, they obtain their final keys. If they are different, they discard their keys.



Alice and Bob can guarantee that there is no error in final keys with high significance level.

Protocol



Calculation complexity

Syndrome (Information reconciliation):

When our error correcting code is LDPC, the calculation of syndrome is not so large

Decoding (Information reconciliation):

When we employ a LDPC code, decoding can be done efficiently when block length is around $2^{16} = 65536$.

Universal2 hash function (Privacy amplification & Error verification):

When it is given by using Toeplitz matrix, its calculation complexity is $O(m \log m)$ when m is the input length.

One block of PV can be composed of several blocks of error correction.

Asymptotic key generation under iid assumption

$$H[P_{E'}, \nu]$$

$$:= - \int_{-\infty}^{\infty} \left(\Phi\left(\frac{x}{\sqrt{\nu}}\right) \log \Phi\left(\frac{x}{\sqrt{\nu}}\right) + (1 - \Phi\left(\frac{x}{\sqrt{\nu}}\right)) \log(1 - \Phi\left(\frac{x}{\sqrt{\nu}}\right)) \right) P_{E'}(dx)$$

Theorem

Assume that injected noise is subject to iid and there exists CDF F such that

$$\Phi_{\frac{a_B^2 b_E^2}{a_E^2 + b_E^2}} = F_Y * F, \quad \Phi_{\nu} : \text{CDF of Gaussian distribution of variance } \nu \text{ and mean } 0$$

 The asymptotic key generation rate of our protocol is

$$H[P_{E'}, \nu_{B|E'}] - H(B' | A)[P_{B'A}], \quad \nu_{B|E'} := \frac{a_B^2 b_E^2}{a_E^2 + b_E^2} + b_B^2$$

Sketch of proof

Z : Random variable whose CDF is F

$$F * F_{E'} = F * \left(\Phi_{\frac{a_B^2 a_E^2}{a_E^2 + b_E^2}} * F_Y \right)$$

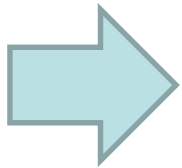
$$= \Phi_{\frac{a_B^2 a_E^2}{a_E^2 + b_E^2}} * F_Y * F = \Phi_{\frac{a_B^2 a_E^2}{a_E^2 + b_E^2}} * \Phi_{\frac{a_B^2 b_E^2}{a_E^2 + b_E^2}} = \Phi_{a_B^2}$$

$Z + E'$ is subject to the same distribution as $a_B A$

We have the following Markovian chain

$$E' - (Z + E') - B - B'$$

$$E' - A - B - B'$$



$$I(B'; A) - I(B'; E') = I(B'; A | E')$$

$$= H[P_{E'}, \nu_{B|E'}] - H(B' | A)[P_{B', A}]$$

(*)

Derivation of (*)

$$\begin{aligned} I(B'; A) - I(B'; E') &= I(B'; A | E') \\ &= I(B'; Z + E' | E') = I(B'; Z | E') \\ &= H(\text{sgn}(E' + Z + Y + b_B X_1) | E') \\ &\quad - H(\text{sgn}(E' + Z + Y + b_B X_1) | E' Z) \\ &= H(\text{sgn}(E' + Z + Y + b_B X_1) | E') \\ &\quad - H(\text{sgn}(E' + Z + Y + b_B X_1) | E' + Z) \\ &= H(\text{sgn}(B) | E') - H(\text{sgn}(B) | A) \\ &= H[P_{E'}, \nu_{B|E'}] - H(B' | A)[P_{B'A}] \end{aligned}$$

Gaussian noise case

Theorem

Assume that \mathbf{Y} is subject to Gaussian distribution with variance ν_0

The asymptotic key generation rate of our protocol is

$$R_2 := \left(h\left(\frac{\alpha_B + \alpha_E + 1}{\alpha_B \alpha_E + \alpha_Y (\alpha_E + 1)}\right) - h\left(\frac{\alpha_Y + 1}{\alpha_B}\right) \right)_+$$

where

$$\alpha_B := \frac{a_B^2}{b_B^2}, \alpha_E := \frac{a_E^2}{b_E^2}, \alpha_Y := \frac{\nu_0}{b_B^2}$$

$$h(\nu) := \int_{-\infty}^{\infty} h_2\left(\Phi_1\left(\frac{x}{\sqrt{\nu}}\right)\right) e^{-\frac{x^2}{2}} dx$$

Gaussian noise case

Theorem

Assume that \mathbf{Y} is subject to Gaussian distribution with variance ν_0

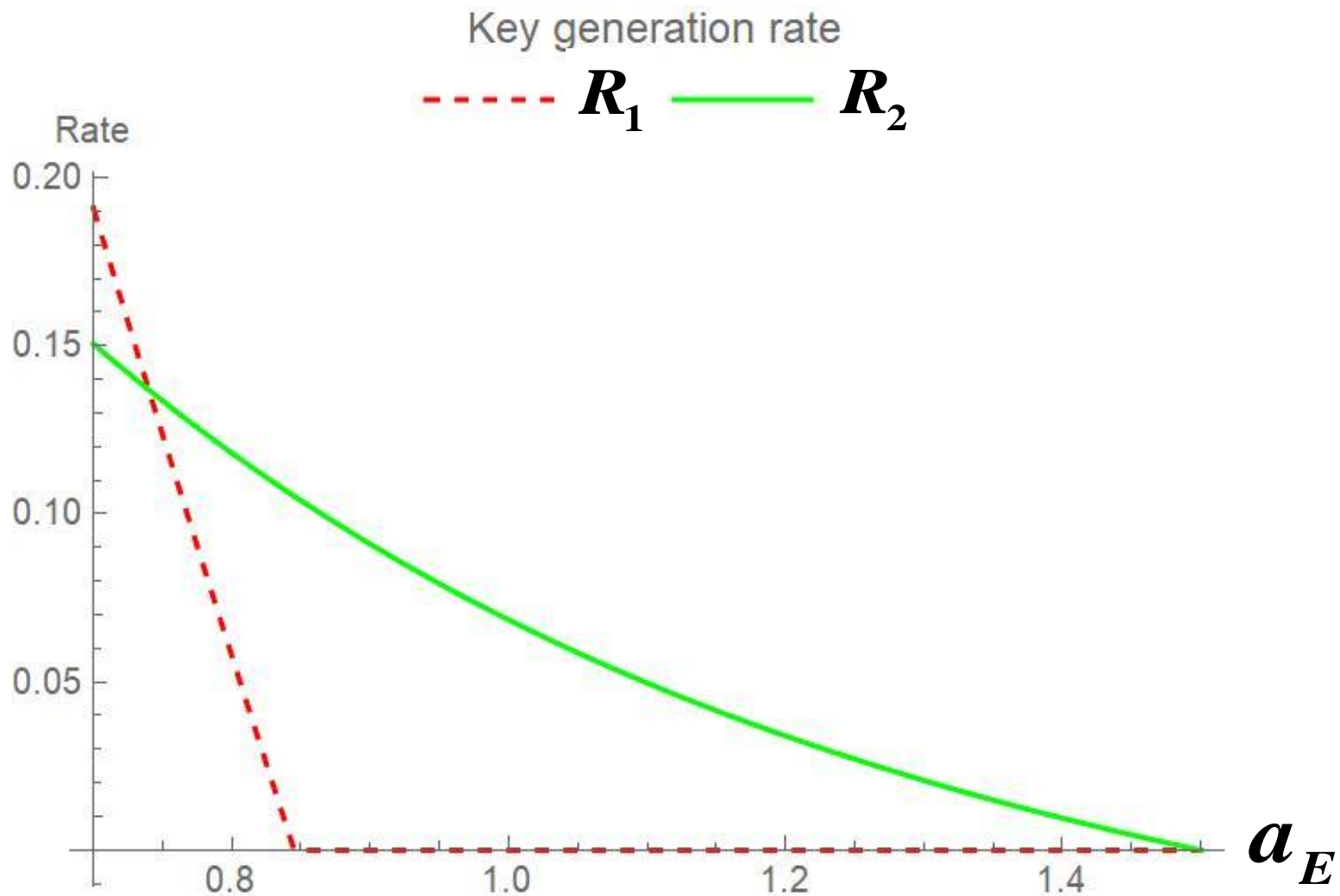
The one-way asymptotic key generation rate is

$$R_1 := \left(\frac{1}{2} \log\left(1 + \frac{\alpha_B}{\alpha_Y + 1}\right) - \frac{1}{2} \log(1 + \alpha_E) \right)_+$$

where

$$\alpha_B := \frac{a_B^2}{b_B^2}, \alpha_E := \frac{a_E^2}{b_E^2}, \alpha_Y := \frac{\nu_0}{b_B^2}$$

Numerical comparison



$$b_E = b_B = 0.5, a_B = 1, v_0 = 0.1$$

How to decide the sacrificed length

$$\psi_{\nu,t}(x) := \left(\left(\Phi_1\left(\frac{x}{\sqrt{\nu}}\right) \right)^{\frac{1}{1-t}} + \left(1 - \Phi_1\left(\frac{x}{\sqrt{\nu}}\right) \right)^{\frac{1}{1-t}} \right)^{1-t}$$

$$\hat{\nu}_3 := \frac{(a_B - \delta)^2 b_E^2}{a_E^2 + b_E^2} + b_B^2$$

$$\hat{\eta}(t) := \frac{n}{l} \sum_{i=1}^l G_{\hat{\nu}_3}^{-1} \left[\frac{1}{t} \log \psi_{\hat{\nu}_3,t} \right] (B_j)$$

$$\delta_2 := 3\delta \left(1 + \frac{\left\| G_{\hat{\nu}_3}^{-1} \left[\frac{1}{t} \log \psi_{\hat{\nu}_3,t} \right] \right\|_2}{\sqrt{2\hat{a}_B} \sqrt{\pi\hat{\nu}_3}} \right)$$

G_ν : Gaussian convolution with variance ν

How to decide the sacrificed length

Sacrificed bit length in PV

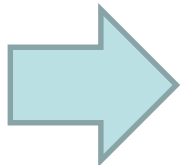
$$m_1 := n + \hat{\eta}(t) + n\delta_2 + \frac{n\varepsilon}{t}$$

Theorem

Amount of information leakage based on variational distance

$$d(K : E | RG)$$

$$\leq 3e^{-\varepsilon n} + 2\left(\frac{4\left\|G_{\hat{v}_3}^{-1}\left[\frac{1}{t}\log\psi_{\hat{v}_3,t}\right]\right\|_2^2}{l\delta\sqrt{2\pi v_{B|E}}}\right) + \exp\left(-\frac{2l\delta^2 n^2}{(n+1)(n+l)}\right) + 2\frac{2a_B + b_B + v_Y}{l\delta}$$



Soundness

Asymptotic evaluation

Assume IID assumption

Asymptotic rate of the sacrificed bit length

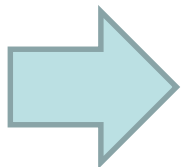
$$\frac{m_1}{n} \rightarrow 1 - H(P_{E'} | v_{B|E'}) \text{ as } n \rightarrow \infty, t \rightarrow 0$$

Asymptotic rate of information reconciliation

$$1 - H(B' | A)$$

Asymptotic key generation rate

$$\begin{aligned} & 1 - H(B' | A) - (1 - H(P_{E'} | v_{B|E'})) \\ &= H(P_{E'} | v_{B|E'}) - H(B' | A) \end{aligned}$$



Completeness

Conclusion

- We have proposed a protocol to generate secure key via wireless communication only under the spatial condition between Alice and Eve and local Gaussian noise in Eve's detector.
- Our analysis can be applied to the case when Eve can generate artificial noise.
- We have also derived a quantitative evaluation of leaked information.

THANK YOU FOR
YOUR ATTENTION.